U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE U.S. DESIGNATED/ELECTED OFFICES (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371	ATTORNEY DOCKET NO.: 40124/00601

Commissioner for Patents
P.O. Box 2327
Arlington, VA 22202

Box: Patent Application

Certificate of Mailing
I hereby certify that this correspondence is being deposited with U.S. Postal Services as Express Mail No. EL 869 561 673 US in an envelope addressed to:
Commissioner for Patents
P.O. Box 2327
Arlington, VA 22202
By: Lesla Ramos Date: 3/1/02

Customer No.: 30636
PATENT TRADEMARK OFFICE

Sir:

Applicants herewith submit to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

International Application No.:	**PCT/EP00/08516**
International Filing Date:	**31 August 2000**
Priority Date Claimed:	**02 September 1999**
Applicant(s) for DO/EO/US:	**VON ALTROCK, Constantin; HEPP, Hanns Michael and PRASCHINGER, Johann**
Title of Invention:	**EXPERT SYSTEM**

Applicants' Statements:

1. This is a FIRST submission of items concerning a filing under 35 U.S.C. 371.
2. This express request to begin national examination procedures (35 U.S.C. 371(f)).
3. A copy of the International Application as filed has been transmitted by the International Bureau.
4. Amendments to the claims of the International Application under PCT Article 19 have not been made and will not be made.

Applicants hereby submit following items:

1. English language translation of the International Application.
2. Substitute Specification along with a Marked Up Version of the Substitute Specification.
3. Translation of Additional Claims.

4. Drawings.

5. Declaration of the Inventor(s) (unexecuted).

6. Preliminary Amendment.

7. Written Opinion along with English translation.

8. International Search Report.

9. International Preliminary Examination Report along with English translation.

10. Form PCT/RO/101.

11. Return Receipt Postcard.

12. A deposit account charge authorization: Please charge the deposit account of **Fay Kaplun & Marcin, LLP,** deposit account no. **50-1492** in the amount of **$890.00** for the filing fee calculated as shown below:

	NUMBER FILED		NUMBER EXTRA*	RATE ($)	FEE ($)
BASIC FEE					890.00
TOTAL CLAIMS	16	- 20 =	0	18.00	
INDEPENDENT CLAIMS	3	- 3 =	0	84.00	
MULTIPLE DEPENDENT CLAIM PRESENT				280.00	
*Number extra must be zero or larger				TOTAL	890.00
If applicant is a small entity under 37 C.F.R. §§ 1.9 and 1.27, then divide total fee by 2, and enter amount here.				SMALL ENTITY TOTAL	

13. A copy of this transmittal letter is enclosed for the following Deposit Account purposes:

The Commissioner is hereby authorized to charge the payment of any additional fees associated with this communication or arising during the pendency of this application, with the exception of the issue fee, to the Deposit Account of **Fay Kaplun & Marcin, LLP No. 50-1492**.

When payment of the issue fee has previously been provided or authorized, the Commissioner is hereby authorized to charge any post issuance fees required, except for patent maintenance fees, to the Deposit Account of **Fay Kaplun & Marcin, LLP No. 50-1492**.

Dated: March 1, 2002 By: _____
Oleg F. Kaplun (Reg. No. 45,559)

Fay Kaplun & Marcin, LLP
100 Maiden Lane, 17th Floor
New York, NY 10038
(212) 898-8870 (phone)
(212) 208-6819 (facsimile)

[40124/00601]

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s)	:	VON ALTROCK et al.
Serial No.	:	To Be Assigned
Filed	:	Herewith
For	:	EXPERT SYSTEM
Art Unit	:	To Be Assigned
Examiner	:	To Be Assigned

Assistant Commissioner
for Patents
P.O. BOX 2327
Arlington, VA 22202

PRELIMINARY AMENDMENT AND
37 C.F.R. § 1.125 SUBSTITUTE SPECIFICATION STATEMENT

SIR:

Please amend the above-identified application before examination, as set forth below.

IN THE SPECIFICATION AND ABSTRACT:

In accordance with 37 C.F.R. § 1.121(b)(3), a Substitute Specification (including the Abstract, but without claims) accompanies this response. It is respectfully requested that the Substitute Specification (including Abstract) be entered to replace the Specification of record.

IN THE CLAIMS:

Without prejudice, please cancel original claims 1 to 3 and substitute claims 1 to 3, and please add new claims 4 – 19 as follows:

--4. (New) For use in a computer controlled transaction system, a method for determining an extent of a risk of a current transaction in the computer controlled transaction system being fraudulent, comprising the steps of:

receiving data on the current transaction data in a prediction model;

identifying a means of payment used in preceding transactions in the prediction model;

EL 869 561 673 US

combining a limit with a value in the prediction model for generating an output value that depicts the extent of the risk of the current transaction being fraudulent; and

initiating reactions to the current transaction;

wherein the reactions have different magnitudes corresponding to the output value that depicts the extent of the risk of the current transaction being fraudulent;

wherein the limit is essentially based on expert rules and the limit being specific for a type of transaction;

wherein the value is essentially based on a time series analysis of the preceding transactions with regard to the means of payment and the value being specific for the current transaction; and

wherein combining the limit and the value is performed in a floating manner so that the output value varies in accordance with an extent of the risk of the current transaction being fraudulent.

5. (New) The method of claim 4, wherein the expert rules concern parameters which occur in statistically significant cumulative manner during fraudulent transactions.

6. (New) The method of claim 5, wherein the parameters relate to at least one element selected from the group consisting of an origin of a payment, an origin of a user, a branch of the current transaction, a beneficiary of the current transaction, a magnitude of the current transaction and a value of the current transaction.

7. (New) The method of claim 4, wherein the time series analysis is implemented in the form of fuzzy logic rules.

8. (New) The method of claim 4, wherein the expert rules are implemented in the form of fuzzy logic rules.

9. (New) The method of claim 8, wherein the expert rules are implemented in the form of fuzzy logic rules.

10. (New) A system for determining an extent of a risk of a current transaction in a computer controlled transaction system being fraudulent, comprising:

a prediction model module;

a module for receiving data on the current transaction data, the module for receiving data being in the prediction model module;

a module for identifying a means of payment used in preceding transactions, the module for identifying being in the prediction model module;

a module for combining a limit with a value and for generating an output value that depicts the extent of the risk of the current transaction being fraudulent, the module for combining the limit with the value and for generating the output value being in the prediction model module; and

a module for initiating reactions to the current transaction;

wherein the reactions have different magnitudes corresponding to the output value that depicts the extent of the risk of the current transaction being fraudulent;

wherein the limit is essentially based on expert rules and the limit being specific for a type of transaction;

wherein the value is essentially based on a time series analysis of the preceding transactions with regard to the means of payment and the value being specific for the current transaction; and

wherein combining the limit and the value is performed in a floating manner so that the output value varies in accordance with an extent of the risk of the current transaction being fraudulent.

11. (New) The system of claim 10, wherein the expert rules concern parameters which occur in statistically significant cumulative manner during fraudulent transactions.

12. (New) The system of claim 11, wherein the parameters relate to at least one element selected from the group consisting of an origin of a payment, an origin of a user, a branch of the current transaction, a beneficiary of the current transaction, a magnitude of the current transaction and a value of the current transaction.

13. (New) The system of claim 10, wherein the time series analysis is implemented in the form of fuzzy logic rules.

14. (New) The system of claim 10, wherein the expert rules are implemented in the form of fuzzy logic rules.

15. (New) The system of claim 14, wherein the expert rules are implemented in the form of fuzzy logic rules.

16. (New) A method which is implemented on a computer and which is provided for identifying and determining fraudulent transaction data in a computer-controlled transaction processing system with a prediction model for receiving current transaction data, for processing the current transaction data, and for outputting at least one output value that depicts a probability of a fraudulent transaction, wherein, on the basis of stored data, for

a time series analysis, and

expert rules concerning parameters which occur in a statistically significant cumulative manner during fraudulent transactions, especially with respect to the origin of the means of payment or user, to the branch and to the beneficiary of the transaction, as well as to the magnitude or value of the transaction, the evaluation is carried out by means of the prediction model with respect to the risk of the current transaction being fraudulent, and a corresponding output value is generated,

wherein the prediction model combines a limit, which is essentially based on the expert rules and which is specific for the type of transaction, with a value, which is essentially based on the time series analysis of preceding transactions with regard to the same means of payment and which is specific for the current transaction, in order to generate the output value, and

wherein the combination is carried out in a floating manner so that output values can be generated which vary according to the extent of the suspicion of misuse and which can be used to initiate reactions of different magnitude to the current transaction request instead of the definition of only one risk-threshold for authorization of the transaction.

17. (New) The method of claim 16, wherein the time series analysis is implemented in the form of fuzzy logic rules.

18. (New) The method of claim 16, wherein the expert rules are implemented in the form of fuzzy logic rules.

19. (New) The method of claim 18, wherein the expert rules are implemented in the form of fuzzy logic rules.--.

Remarks

This Preliminary Amendment cancels without prejudice original claims 1 to 3 and substitute claims 1 to 3 in the underlying PCT Application No. PCT/EP00/08516, and adds without prejudice new claims 4 to 19. The new claims conform the claims to U.S. Patent and Trademark Office rules and do not add new matter to the application.

In accordance with 37 C.F.R. § 1.121(b)(3), the Substitute Specification (including the Abstract, but without the claims) contains no new matter. The amendments reflected in the Substitute Specification (including Abstract) are to conform the Specification and Abstract to U.S. Patent and Trademark Office rules or to correct informalities. As required by 37 C.F.R. § 1.121(b)(3)(iii) and § 1.125(b)(2), a Marked Up Version Of The Substitute Specification comparing the Specification of record and the Substitute Specification also accompanies this Preliminary Amendment. In the Marked Up Version, shading indicates added text and brackets indicated deleted text. Approval and entry of the Substitute Specification (including Abstract) is respectfully requested.

The underlying PCT Application No. PCT/EP00/08516 includes an International Search Report, with a mailing date of March 13, 2001. The Search Report includes a list of documents that were uncovered in the underlying PCT Application. A copy of the Search Report accompanies this Preliminary Amendment.

The underlying PCT application also includes an International Preliminary Examination Report, dated February 4, 2002, and an annex. An English translation of the International Preliminary Examination Report and the annex accompanies this Preliminary Amendment.

Applicants assert that the subject matter of the present application is new, non-obvious, and useful. Prompt consideration and allowance of the application are respectfully requested.

Respectfully Submitted,

Dated: March 1, 2002

By: _____
Oleg F. Kaplun, Reg. No. 45,559

Fay Kaplun & Marcin, LLP
100 Maiden Lane, 17th Floor
New York, NY 10038
Tel: 212-898-8870
Fax: 212-208-6819

MARKED UP VERSION OF SUBSTITUTE SPECIFICATION

EXPERT SYSTEM

FIELD OF THE INVENTION

[0001] The present invention relates to the detection of the fraudulent use of customer accounts and account numbers, including, for example, transactions with credit cards. The present invention in particular relates to an automated fraud detection system and a method using a prediction model for the pattern recognition and classification so as to pick out transactions having a high likelihood of fraud. In the following discussion, the term "credit card" will be used for descriptiveness purposes; the here discussed methods and fundamentals, however, apply as well to other kinds of electronic payment systems, such as, for example, customer credit cards, automated~~machine-~~ machine-readable cash cards and telephone cards.

BACKGROUND INFORMATION

[0002] The establishments issuing credit cards have at all times tried to restrict their losses caused by fraud in that the fraudulent use of the card is indicated before the card holder has notified a lost or stolen card.

[0003] An effective model for the fraud detection was supposed to result in high catch rates at a low impediment of legal transactions in the real time operation. It was supposed to be able to adapt to changing fraud methods and patterns, and was supposed to have an integrated learning capacity supporting this capacity of adaptation.

[0004] The~~prior published specification~~ WO-A-8 906 398 ~~describes~~is believed to describe an element for the analysis of a transaction by means of data processing: in that only that data is extracted, which ~~is~~may be useful for the analysis of the transaction; in that signals are cancelled corresponding to a transaction which is presumed to match with a set of predetermined rules; in that it is filtered so as to eliminate non-significant modifications of the transaction to be analyzed; and in that signals are classified into one or several classes according to a predetermined criterion. ~~This~~It is believed that this element is suited for the application of issuing payment authorizations to credit card users.

[0005] A further ~~specification,~~reference, EP-A-0 418 144, ~~describes~~is believed to describe a method for restricting the risks associated with a computer-assisted transaction, in that the transaction request ~~is~~may be compared to predetermined statistical data, which seems to be representative of a risk score of a non-conform use. The statistical data describes the mean number or the quantity of transactions performed during the sequence of successive periods of time, and is derived in that the time is divided into successive, non-equal periods, the duration of which are selected in a manner that the likelihood of a performed transaction or the mean amount for each single period of time are substantially equal.

[0006] ~~From EP-0 669 032, a~~The EP-0 669 032 is believed to describe fraud detection method implemented on a computer, and a corresponding hardware ~~are known~~, which includes means for prediction models. Current transaction data is received and processed, which then results in a plurality of output values containing a hit value representing the likelihood for a fraudulent transaction.

[0007] ~~This method known in the prior art~~It is believed that this method requires several steps, which have to be carried out prior to the processing steps for the current data, namely:

a. generating a user profile for each individual of a plurality of users out of an enormous number of variables relative to previous transactions, and of personal user data containing for each user values out of a plurality of user variables, each user profile defining a pattern for the transaction history of a user;

b. deriving variables concerning proven previous fraud in that data of previous transactions are preprocessed, these values containing a plurality of previous transactions for a plurality of transaction variables;

c. training of means for prediction models with said user profiles and said variables concerning previous fraud, so as to obtain a prediction model; and

d. storing said obtained prediction model in the computer.

[0008] Then, the processing of the current data is carried out in that

e. the current transaction data for a current transaction of a user is received;

f. the user data concerning the user, is received;

g. the user profile associated with the user, is received;

h. the obtained current transaction data, user data and the user profile are preprocessed so as to derive variables relative to a current fraud for the current transaction;

i. the likelihood of fraud in the current transaction is determined in that the prediction model is applied to the current fraud-related variables; and

j. an output signal is emitted from the means for the prediction model, which signal indicates the likelihood of fraud for the current transaction.

[0009] This system supports on a neuronal network for training the means for the prediction model. Said training is supposed to mainly change the means for the prediction model so as to keep the prevention of legal transactions low, and to improve the performance of the system for the detection of fraud.

[0010] Hereby, the system supports on a set of fixed (yet variable) values representing various aspects of the transaction. These values are differently weighted in processing, and one important function of the training based on the neuronal network, is the variation of said weighting, basically resulting in a "learning" capacity for this system. Such~~known~~ neuronal networks represent a linking of "neurons" in the meaning of simple mathematical transfer functions. For generating a "learning capacity" here, a corresponding algorithm is used – e.g.

according to EP 0 669 032, for adapting the "weights" with the data rating in the neuronal network.

[0011] In spite of all that, the system for combining the different parameters and data, employs usual logic algorithms and functional relationships for obtaining the hit value. For each current transaction, it carries out a calculation based on conventional logic, views the results (later), and varies, if necessary, the algorithm.

SUMMARY OF THE INVENTION

[0014] ~~It is desirable~~An object of an exemplary embodiment and/or exemplary method of the present invention is to create an automated system which uses the available information, e.g. on the card holder, merchants and shops for monitoring transactions and picking out these which are probably fraudulent, and which is able of thereby discovering a relatively higher portion of cases of frauds at a relatively lower prevention of legal transactions. ~~Such~~A further object of an exemplary embodiment and/or exemplary method of the present invention is to provide a system that should preferably also be capable of dealing in a fast real time operation with a large number of variables independent of each other, and should feature the capacity of redeveloping the basic system model as new patterns for upcoming fraud behavior.

[0015] It is believed that these objects may be achieved with a method for use in a computer controlled transaction system for determining an extent of a risk of a current transaction in the computer controlled transaction system being fraudulent according to claim 4, a system for determining an extent of a risk of a current ~~The invention accordingly relates to~~transaction in a computer controlled transaction system being fraudulent according to claim 10 and a computer-implemented method for identifying and determining fraudulent transaction data according to the features of claim 16.

[0014] ~~To some extent, the invention uses features known from EP 0 669 032.~~ Reference is~~therefore~~ made to the complete scope to EP 0 669 032 which is hereby incorporated by reference.

[0015] As can be seen from the following ~~description, there exist, however,~~ description where an exemplary embodiment of the present invention is described with reference to the method of the EP 0 669 032 to emphasize the difference of this exemplary embodiment of the present~~major differences betweenthe~~ invention and this ~~prior art, residing~~method, there exist ~~in the basic approach and in the corresponding basic structure, as well as in various details of the data generation and processing.~~

[0016] ~~An~~It is believed that an essential difference results from the fact that according to an aspect of this exemplary embodiment of the present invention ~~does not use~~there is no use of a user profile as a part of the prediction model. Instead, this exemplary embodiment of the present invention works with a combination of expert rules, for one, and an analysis of preceding operations of using the payment means, for another, which is used for the transaction to be currently evaluated.

[0017] ~~Comparable to the initially mentioned prior art,~~According to another aspect of an exemplary embodiment of the present invention, the expert rules concern a selection of typical elements of an individual transaction based on experience values, i.e. the analysis of past cases of misuse, which elements are indicative for an increased risk of misuse. According to yet another aspect of an exemplary embodiment of the present invention, the origin of the payment means is in particular relevant (e.g. the card), the branch and the person beneficiary of the payment to be authorized, and the payment amount.

[0018] ~~The~~According to yet another aspect of an exemplary embodiment of the present invention, the analysis of preceding events of use of the same payment means preferably comprises the latest events, for example, the last five to twenty transactions (this could, however, also go further back).

[0019] In contrast to the ~~prior art as per EP 0 669 032, the invention preferably does not use~~method of the EP 0 669 032, according to yet another aspect of an exemplary embodiment of the present invention, there is no use of a conventional neuronal network in combination with a learning algorithm.

[0020] The method and system according to exemplary embodiments of the present invention uses fuzzy logic for determining whether a certain transaction has to be considered as being fraudulent.

[0021] In the decision system preferred according to yet another aspect of an exemplary embodiment of the present invention, the expert rules, as well as the rules functionally corresponding to the prior art neuronal network, ~~are~~may be memorized for the descriptive statistics as fuzzy rules, and therewith do not differ in the calculation method, but in the gaining method.

[0022] The expert knowledge ~~is~~may directly be formulated as fuzzy rules. These define a limit for each transaction type that corresponds to the (user-specific) "risk readiness".

[0023] The information from the use history of the payment means ~~is~~may be likewise transformed into fuzzy rules by means of a "NeuroFuzzy module". The NeuroFuzzy module ~~uses~~may use a modification of that training algorithm, which ~~is~~may also be used in most neuronal networks, namely the Error Backpropagation algorithm ~~to a large extent~~ described in the literature. Since in this way the information from past data (hence that, what is, for example, memorized in the weights of the trained neuronal network according to EP 0 669 032) is available as readable and interpretable/modifiable fuzzy rules, this information can be completed, verified and extended in any manner. With respect to the input and output data, the "neuronally" generated fuzzy rules can use the same variables as the expert rules.

[0024] The "neuronally" generated fuzzy rules according to yet another aspect of an exemplary embodiment of the present invention, are preferably based on an analysis of preceding transactions with respect to such factors as the average transaction amount, the portion of cash disbursements, the portion of foreign jobs, of travel cost use, the previous occurrence of suspicious cases, etc., and with respect to "dynamic" criteria such as, for example, the current exhaustion of the limit of the credit card concerned. The result of this analysis is also designated as "time series". This rule system thus assesses a dynamic risk for each transaction in the form of a "bonus" or a "malus".

[0025] Thus, it is believed that the invention permits the merging of statistical models with expert knowledge. Instead of simply calculating for each event, as it is the case with ~~prior art,~~the above-mentioned references, a fraud probability, the limit defined for each transaction type, is floatingly combined with the dynamic risk ("bonus" or "malus") of the specific current transaction to a (floating) transaction limit.

[0026] ~~This~~It is believed that this enables various differentiated treatments of "eye-catching" transactions, e.g. the immediate interlock, or instead, the remittance for an individual check, e.g. through a person in charge.

[0027] In the ~~prior art,~~above-mentioned references, a transaction lying above the risk threshold normally is ~~stopped; the prior art basically only knows~~stopped. Basically, according to these references, there is only the release or interlock as a result of the check. The method system according to yet another aspect of an exemplary embodiment of the present invention instead enables gradual reactions; for example, a suspicious case can be generated (and therewith enter into the "time series" for this credit card, which will be referred to for future transactions), although the current transaction is being authorized. In case of a stronger suspicion, a re-check (referral) of the current transaction would be initiated (prior to the possible authorization thereof); with a still stronger suspicion, the transaction would be rejected (decline).

[0028] Substantial differences ~~to the prior art also~~between the above references and a method/system according to an exemplary embodiment of the present invention result with respect to the model formation, hence, the generation and recognition of misuse patterns (fraud patterns).

[0029] ~~The prior art is~~It is believed that the above references are based on a "passive data gain". In other words, exclusively already present past data is referred to for the model formation. This means that, for being able to recognize a fraud pattern in the model at all, (a) a sufficiently long time must have elapsed, so that the fraud messages have already come back

(in most cases only after the customers have read their statement of accounts), (b) enough cases for a secure training must be given (a neuronal network functions only in this case / there exist fraud cases which are very rare but cause a high individual damage, and which are only very difficult to cover in the model, (c) an immunization of the authorization operation is only possible at all after laborious manual retraining.

[0030] The data gain according to yet another aspect of an exemplary embodiment of the present invention, however, is "active". If the first suspicious factors of a new fraud pattern arise, then new rules will be defined immediately initiating an investigation of exactly these cases by actively contacting the customers. Thus, many secured data will be available within a few hours in the ideal case as to whether a new fraud pattern has actually arisen, and how it differentiates from other patterns. This analysis (it makes no difference by means of which method) namely can only then be carried out when enough secured data is present.

[0031] ~~The~~It is believed that the methods of the~~prior art~~ model establishment in accordance with a reference mentioned above leads to the fact that the experience of human analysts cannot sufficiently be used, and expectations as to future fraud patterns cannot gain entry. In ~~the prior art,~~these methods, the neuronal network virtually constitutes a "black box" of fixed, rigid criteria, which still are only modified "automatically" with respect to their "weights", hence, as the result of algorithms in turn fixed beforehand. As far as expert rules are used at all together with neuronal networks, neuronal network and expert rules run independently ~~side-by-side.~~side-by-side. Through the NeuroFuzzy approach according to yet another aspect of an exemplary embodiment of the present invention, the predictive model trained with data, is no longer a black box, but is generated in the form of fuzzy rules. These can be directly interpreted and modified by experts.

[0032] The floating transaction limits according to yet another aspect of an exemplary embodiment of the present invention permit an efficient combination of "hard facts" and "soft facts". ~~This~~It is believed that this enables the "soft" and "hard" facts to be modeled in a consistent and cooperative way. With the~~prior art~~ "black box" approach of the above references, this is of no importance, since there, no knowledge-based modelling takes place.

With the invention which enables and preferably also provides that an automatic model formation and human expertise are combined in the running operation, this is very relevant.

[0033] The invention will be explained in more detail in the following by means of an exemplary embodiment comprising configurations of the inventive basic principle particularly preferred at present.

BRIEF DESCRIPTION OF THE DRAWINGS

[0034] ~~The~~Figure 1 shows an exemplary embodiment of a principal information exchange performed in an exemplary embodiment of the method and system of the present invention.

Figure 2 shows an exemplary embodiment a data flow with presumed or recognized misuse cases occurring in an exemplary embodiment of the method and system of the present invention.

Figure 3 shows another exemplary embodiment a data flow occurring in an exemplary embodiment of the method and system of the present invention.

Figure 4 shows yet another exemplary embodiment a data flow occurring in an exemplary embodiment of the method and system of the present invention.

Figure 5 shows an exemplary embodiment of a structure for this fuzzy system having input interfaces, rule blocks and output interfaces in an exemplary embodiment of the method and system of the present invention.

DETAILED DESCRIPTION

[0035] An exemplary embodiment of the present invention relates to an authorization system for credit card transactions, and therewith to a basic constellation similar to that of the initially discussed ~~state of the art.~~references. From an existing network comprising points of

use for the credit cards usable in the system, come authorization requests which have to be handled and answered in real time.

[0036] The handling of the authorization requests takes place in the inventively configured authorization system schematically shown in the Figures 1 through 4.

[0037] In the exemplary embodiment, the system comprises several computers but can of course also be realized on a central computer or by means of a computer network.

[0038] In the ~~example,~~exemplary embodiment, the system comprises a "tandem" computer with a database A, an "SGI" server (SQL server) with a database B, and a "host system" with a database C.

[0039] On the tandem computer, a software ~~is~~may be implemented serving for data transfer, data reprocessing (criteria derivation), time series calculations and time series updates, etc., as will become clear later. Moreover, the inventive decision logic is implemented on the tandem computer, including fuzzy expert rules and NeuroFuzzy models, and making the decision on authorization requests. The software implemented on the tandem computer in summary will be designated "NeuroFuzzy Interference Machine" (NFI) in the following.

[0040] The SGI server, if the case may be in conjunction with a corresponding number of PC clients, serves in particular for the implementation of the software for the "Investigation Workflow" (IW) for the follow-up on cases of suspicion, and for the "Online Data Mining Module" (ODMM), as will be explained later.

[0041] The host system contains and receives the essential historic and current data as to payment means and user, required for the treatment of the authorization requests.

Figure 1 shows an exemplary embodiment of a principal information exchange ~~as follows:~~

[0042] performed in an exemplary embodiment of the method and system of the present invention as follows: The authorization system obtains data (1) for a cardholder file from database [C] of the host system. With a modification of the data of the cardholder file, only the data of a card number relevant for the authorization is transferred to the authorization system. Events such as card interlocks having a high priority, are immediately transferred, others having a low priority, are transferred only much later. The data transfer (update) ~~takes~~may take place hourly.

[0043] The SGI server receives (2), via the existing network, the authorization requests from the authorization tandem computer provided with the NFI-initiated action (same is comprised of: case importance, case class, case threshold, referral decision, risk score, limit and action code), as well as the current time series information. (The real time requests necessary for this purpose are in the range of minutes. The overall information as to an authorization request is compressed to a message by the NFI, which message is then transferred to the SGI server).

[0044] The SGI server further receives from the host system any posting information, misuse information and, if the case may be, card-holder main data, which cannot be extracted from the cardholder file (3). The database of the SGI server [B] stores this data as long as required, depending on the storage expansion. The SGI server lodges the server component, be it of the Supervisory Workflow (ODMM) or also of the Investigation Workflow (IW).

[0045] Figure 2 shows an exemplary embodiment of the data flow with presumed or recognized misuse cases.

[0046] The Investigation Workflow (IW) (6) serves for the treatment, in particular by means of staff members (Call Center), of recognized and presumed fraud cases.

[0047] In the Call Center, it is ascertained whether the presumed cases of misuse actually are cases of misuse. A corresponding information (7) to the SGI server takes place.

[0048] Apart from this main task, the SGI server fulfils still another main task:

[0049] The SGI server database stores the data necessary for the discovery of new fraud patterns, and processes ~~same~~it for an analysis by the Online Data Mining Module (ODMM). For this purpose, the misuse-relevant data is buffered in database [B]. In the Fraud Supervisory Center, new fraud rules are then defined by means of this information (4), and the existing fraud rules are continuously checked for their efficiency.

[0050] The correspondingly modified fraud rules in the form of a file are then transferred from the Fraud Supervisory Center to the authorization computer (5). For doing this, the file is brought to the SGI server from the PC. On the SGI server, an automatic job is installed which recognizes when the time stamp of the file has changed, and performs an exchange of said file on the tandem in this case and also communicates to the NFI that has to read-in this file anew.

[0051] Hence, two workflows result *in toto* ~~(Figure 4):~~as may be taken from Figure 4:

1. The Supervisory Workflow ODMM adapts continuously the decision strategy of the prevention system to the changing misuse patterns.

2. The Investigation Workflow IW checks the decisions of the prevention system by individually treating the reported and presumed cases of misuse.

[0052] Both Workflows are indirectly connected via the (mean) operative EDP level. If the decision strategy is modified in the Supervisory Workflow, then other referrals will be generated by the prevention system, which will be investigated in the Investigation Workflow.

[0053] A misuse not timely recognized by the prevention system, as well as an erroneous misuse presumption, is verified by the Investigation Workflow and stored in the database of the SGI server. Hereto accesses the Online Data Mining Module (ODMM) and proposes a corresponding modification of the decision strategy to the fraud experts in the Fraud Supervisory Center.

MARKED UP VERSION OF SUBSTITUTE SPECIFICATION

[0054] The overall calculation, hence the flow of the fuzzy interference through the rule work, as well as the entire profile formation and initialization, is taken over by the NFI itself; an external control is not required. The interface contains further functions for the initialization and configuration of the decision logic (these functions have to be invoked once upon loading of the prevention module), which, however, have not to be invoked per authorization request.

[0055] The SQL database of the authorization computer (Cardholder File) is supplemented by a field "time series". This field stores the last authorization requests to this card number (profile of use) in a compressed form. When an authorization request enters the system, the complete data set of the card is loaded from the database. Here, the binary object "time series" has in addition to be loaded from the database and transferred to the NFI. The binary object profile of card use is then generated in an extremely compressed form, so that is can be efficiently stored in the SQL database for the real time access. Additional computing time by the read-~~read-~~out and re-storage of the card profile upon each authorization request~~,~~ will not cause a noticeable computing effort, since the data set of a card is in any case read out upon each authorization request. After the decision, the NFI updates the time series by the authorization just received. Exactly as the limits updated by the authorization, the updated time series has to be written back into the database, as well.

[0056] Furthermore, the Cardholder File is supplemented by two date fields, in each case one for "no referral until" (this field is set upon a positively answered referral for ensuring that, immediately after a positive ID, the card holder directly receives again a referral on the occasion of the next transaction), and one for "short referral until" (upon an acute suspicion, this date is set so as to forcibly generate a referral with each authorization request up to this date). These fields are set or reset through the authorization system. The data is delivered to the NFI by the authorization system, the NFI evaluates the data and decides whether a referral or decline or, if the case may be, a case shall be generated. Since the NFI, if the case may be, also contains client-dependent rules, the NFI has to recognize the client from the card number.

(A client is, for example, the client of the processing company, for whom the fraud processing is carried out).

[0057] The development component is part of the Supervisory Workflow and a graphical development and analysis software, which is installed on Windows/NT workstations (clients). Hereby, existing computers can be concerned which are also used for other tasks, or a separate computer can be provided.

[0058] Proceeding from the development software, the developer ~~can~~may modify the fuzzy decision system of the tandem. Hereby, the ongoing authorization process is in any case neither stopped, nor disturbed nor decelerated.

[0059] If new fraud patterns become known, then the development component allows to take same into consideration by modification of known and definition of new rules. Thereby, these new rules and modified rules are transferred to the NFI, where the new rules have an instantaneous effect on the authorization behavior.

[0060] All authorization requests are handed over by the tandem to the SGI server via TCP/IP. The SGI server establishes a new record for each authorization request, and fills the same with all necessary information.

[0061] If the case importance of an authorization request is above the case threshold, then the SGI server establishes a case in addition. A case is comprised of an entry in the case table and the associated sub-tables.

[0062] In summary:

[0063] Each message incoming from the tandem describes an authorization request.

[0064] A record is established for each authorization request.

[0065] The case generation is independent of the referrals, i.e., a case may be generated without a referral having been generated, and a referral may be generated without a case being generated.

[0066] This interface is installed on part of the SGI servers. Likewise is the generation of the corresponding entries in the SGI server tables.

[0067] The Investigation Workflow serves for following up the possible fraud cases and referrals. Hereby, the case importance ascertained by the NFI is taken as a basis for the case grading. Whether a referral has been generated for this authorization request or not, is not important for the generation of a case. The case generation works with its own decision logic, which can also contain rules deviating from the fraud rules. Prevention strategies can hereby be tested so to speak, as a "dry run". Therewith, also such cases can be followed up in the Investigation Workflow, in which the suspicion did not suffice for a referral generation.

[0068] Compressed storage of the authorization history ("time series")

[0069] The NFI works with neuronal models which are based on the analysis of previous transactions.

[0070] The problem of such an analysis is that during the treatment of an authorization request, a polling and analysis of past transactions is not possible in real time. Therefore, the NFI has to store a brief history temporarily in a ring buffer. (A ring buffer is a storage having a fixed number of places switched in series. Each newly stored object is pushed into the ring buffer "at the front", thus advancing all objects already present in the ring buffer in each case by one position. The object in the last place thereby completely falls out of the ring buffer.) It is of particular importance here that the time series requires as little storage place as possible (each byte per card results in a net storage place requirement of about 7 megabyte in the database of the authorization computer), and that it is allowed to be read and written as fast and efficiently as possible.

[0071] The time series formation is for this reason based on an algorithm, which generates and updates said ring buffer in such a manner that it is efficient to store and compute. For the storage, a compressed memorization in the converted integer format is used.

[0072] The time series information thereby represents, for example, a condensed history of the last 15 authorization requests, which enables a calculation of dynamic criteria (exhaustion, panic, gas station use, etc.) The time series information in addition permits the assessment of aggregated variables such as: average shopping amount, cashing portion, foreign country portion, travel cost use portion, when has a referral been issued for the last time, and when has a referral been answered for the last time.

[0073] Since the time series information has to be stored (in the ring buffer for each authorization request) 15 times, a compression of the information is particularly important.

[0074] Since the profile is stored in the database as binary object (string format), the individual partial information of each transaction can be coded in the ring buffer as integers of an arbitrary bit length. However, a reasonable division of individual bit lengths to the bytes of the string format has been chosen for keeping the calculation and update of the profiles from becoming computationally not too laborious. Hereby, the shortest possible storage form "exact bit" is not always chosen, rather there results a compromise of storage place requirement minimization and computational performance maximization.

[0075] As to the stored fields in detail:

[0076] Date

[0077] The storage of the date in the minute format enables the simple calculation of time differences in integer arithmetic of a 16-bit digit (with a 16-bit-minute resolution, a maximum of 45 days can be represented, which is sufficient for the calculation of time differences in the profile).

[0078] The 16-bit values resulting with the subtraction of such minute values for the time differences~~,~~ are directly used as input variables of the NFI without any expansive computationally scaling modifications.

[0079] With the maximum storage length of the minute date after a deadline of 24 bits, however, a reset of the profile information has to ensue every 31 years.

[0080] If this entry "date" is equal to "0", then this means that said entry is not yet used in the ring buffer.

[0081] Amount

[0082] Has to be divided by 10 so as to result in the Euro amount. Hereby results an optimized utilization of the 20-bit digit range.

[0083] Deviations in the amount of below Euro 0.10 are unimportant for the misuse prevention, and the maximally representable amount of over Euro 100,000.00 is also sufficient. Requested values of over Euro 100,000.00 are cut down in the ring buffer to Euro 100,000.00.

[0084] MCC

[0085] Contains the branch code of the contractual partner who has requested the authorization.

[0086] ICA

[0087] Describes all issues by means of their ICA numbers.

[0088] Country code

[0089] For the time series inspections, the country code is sufficient for the origin determination. Same is maximally three-digit, therefore 10 bits are sufficient for the representation (according to MC Quick Reference Booklet, October 97).

[0090] POS

[0091] Receives the 5 possible POS Entry modes. 3 bits, it is true, would suffice so as to depict said 5 possible POS Entry Modes, the representation in 4 bits, however, offers arithmetic advantages.

[0092] Status

[0093] Status describes, for example, whether the expiration date was wrong, or whether a CVC problem has arisen, etc.. (On the magnetic card, the card number is extended by a three-digit code (CVC-1). This three-digit code is not calculable. Therewith, a quite good identification of a genuine card is possible by means of this examination.) It is hereby guaranteed that non-authorized requests can be taken into consideration in the profile.

[0094] Fraud Supervisory Workflow

[0095] The Fraud Supervisory Workflow includes all tools which are used for controlling the decision logic and for waiting. In detail, these are the modules:

[0096] Online Data Mining Module

[0097] For the systematic recognition of new misuse patterns, as well as for the continuous check of the hit security of currently defined decision rules.

[0098] Decision logic

[0099] In this module, the decision components are developed, monitored and controlled.

[0100] Analysis NFI

[0101] The analysis NFI serves for testing new decision logics on past scenarios.

[0102] Online Data Mining Module (ODMM)

[0103] The Online Data Mining Module is comprised of a server component on the SQL server, as well as of a client component on a PC. The client component cooperates with the server via Pass-Through Queries and linked tables.

[0104] The ODMM works with tables in which the authorization requests and cases necessary for the analysis are recorded.

[0105] The ODMM Client contains the following information as to each transaction:

[0106] card number (together with the date and time of the transaction, this information serves for the unique allocation of each transaction (key). Since several events (e.g. several authorization requests, misuse messages, answered referrals, etc.) may belong to a transaction, which can take place at different times, the earliest date will always be used here. This corresponds to the logic that the events belonging to this transaction all refer to the first payment request, which has become known in the system.

[0107] Date and time of the transaction

[0108] Amount in Euro

[0109] Type of transaction (authorized or non-authorized transaction; with non-authorized transactions, for example, no authorization request exists, a posting and a misuse message, however, can be present)

[0110] Misuse (has misuse occurred?)

[0111] Referral (has a referral been generated, if yes, how was it answered)

[0112] Information from the authorization request or the posting (branch code, Country Code origin, POS Entry)

[0113] Random number (selection of a sampling quantity)

[0114] The tables supplying this information, are polled by the ODMM Clients via Pass Through Queries.

[0115] The server allocates posterior incoming misuse messages to transactions already entered in the TRX table. The results are likewise updated for the statistic component.

[0116] Systematic search

[0117] The systematic search runs on the server as Pass-Through Query and generates a table comprising rules which are currently not activated, and which would be reasonable to be included. A misuse amount is allocated to each rule, which could have been prevented during the examination period if this rule had been active. For verifying this statement, each rule also contains the ratio of erroneously versus legitimately refused authorization requests (F/P rate), the number of illegitimate referrals, which enable the judgment as to adoption or refusal of the rule. It is possible to filter the rules in advance by indicating a determined misuse amount and F/P rate. With smaller amounts or higher F/P rates, the found rules are blinded out. The weighting between the misuse amount and the F/P rate can be set during the classification. Therewith, it can be fixed anew with each systematic search, of which importance each of the two variables is supposed to be for the examination.

[0118] Rule optimization

[0119] The negatively answered referrals which could not confirm a misuse, serve for the recommendation to deactivate rules as a basis. If a referral is answered negative, then the associated data set will no longer flow into the analysis as a misuse, but as a good transaction. If it turned out then that the rule has not prevented enough misuse and has prevented many good transactions, then it will be proposed to be deactivated. In this analysis, too, the weighting between the misuse amount and the F/P rate can be set. Therewith, it can be fixed anew with each systematic search, of which importance each of the two variables is supposed to be for the examination.

[0120] Decision logic

[0121] The access to the decision logic ensues over the Fraud Supervisory Workflow:

[0122] The block "Fraud Supervisory Workflow" represents the PC networks in the staff SI. These administer decision logics of an arbitrary number, be it for the filing or as intermediate development stages. (The actual data for the decision logics are centrally stored on the SGI server, so that all fraud analysts have access to same. The access to these decision logics takes place by the PCs with the help of the "Fraud Supervisory Workflow" software.) Each of the decision logics is comprised of the three components, lists, time series and rules. By pressing the respective keys, the corresponding editors for the components will open.

[0123] In the productive operation the decision logic "Operation" always runs-. By pressing the key [transfer], the decision logic "Operation" currently developed in the PC, is transferred to the tandems, and is activated.

[0124] The two decision logics for the analysis of scenarios run on the SGI server. By pressing the key [transfer], the decision logic "Test" currently developed in the PC, is transferred to the SGI servers, and is activated.

[0125] Proceeding during the development

[0126] The basic proceeding during the development of decision logics is the following. The decision logic "Operation" runs on the authorization computer. By pressing the key [transfer], the decision logic "Test" will be overwritten with the decision logic "Operation". (Hereby, not a physical overwriting from the tandem to the SGI server is concerned. The SGI servers also dispose of a copy of the decision logic, whereby the overwriting is directly carried out on the SGI servers.)

[0127] The decision logic "Test" can hereby be modified on the PC, and with the assistance of the analysis NFI, the test of modifications takes place by a direct comparison of the "Test" system and the "Operation" system.

[0128] If the modifications carried out on the decision logic "Test" are successful, then the decision logic "Test" will be overwritten with the decision logic "Operation" by pressing the key [transfer]. After the new decision logic has become operational, the proceeding starts anew.

[0129] Each new transaction is provided with a judgment of case worthiness by the NFI machine. An auxiliary module marks a transaction as a case, when said transaction fulfils a case criterion (MCC, ICA, CNT, POS, amount class, case worthiness).

[0130] Optionally, it can be determined how far the history of the transaction and the posting of an event reaches back. A period of 4 – 6 weeks is considered to be reasonable.

[0131] If a transaction belongs to a category of all possible cases, then a new record will be established in the Investigation Workflow-inherent table. This record contains the following single data:

- card number
- transaction data (date/hour, MCC, CNT, ICA, POS, amount)
- case status (is the case new or has it been closed)
- case importance (the case importance FW represents the NFI score)

- case class (the case class indicates why a transaction has become a follow-up case or to which category the transaction belongs. The identification consequently includes indications as to MCC, ICA, CNT, POS, amount class, FW.)
- user name
- date of resubmission
- close status (the close status of a case supplies details on the result of the treatment after closing the case, and may contain the following information: "no fraud", or "no fraud estimated", "fraud confirmation impossible" or "fraud estimated".)

[0132] The card number is the link (pointer) to the past transactions with the same card number on the DBMS of the SGI server. Together with the card number main data, all data are complete for the Fraud Investigation Workflow.

[0133] NFI input variables

[0134] The NFI is integrated into the authorization process over a token protocol. From here, the NFI takes out all input variables, as well as the time series as binary data object (string).

[0135] As a special form of authorizations, the NFI has to interpret the messages on a referral interlock or a referral_until.

[0136] Referral_until: the parameter referral_until (short referral) is used with a misuse suspicion for preventing authorizations. It is manually activated by an authorization.

[0137] The NFI memorizes the referral_until date in the card profile, and checks during the authorization whether the transaction date is smaller than the referral_until date. If this is the case, a referral will always be generated by the NFI.

[0138] The referral_until parameter is transferred for analysis and reconstruction to the SGI computer via the TCP/IP interface as a component of the transaction data set.

[0139] Referral interlock: the referral interlock is used for preventing the further initiation of referrals after a positive identification or after viewing the past transactions. The referral interlock can adopt the conditions "valid" or "not valid". If it is "valid", then a previously set parameter is activated indicating a fixed offset from the current transaction date (e.g., transaction date + 3 days). The referral interlock is always given in the form of a date, until which it shall last. It namely can only be determined at the current moment whether the interlock therewith is valid or not.

[0140] The referral interlock can be activated, for one, proceeding from the Investigation Workflow. For another, the referral interlock can also be indirectly initiated by the authorization service, when a positive identity check has taken place after a referral. After a positive identity check, the authorization service initiates a transaction, which is processed in the NFI. The NFI writes the current referral interlock into the Cardholder File on the authorization computer.

[0141] The case has to be avoided of a referral interlock, as well as the referral_until date both being valid. For this reason, when one value is set (e.g. referral_until), the respective other value is erased (e.g. referral interlock).

[0142] Internal output variables

[0143] If all input variables are present, which are used by the NFI, then the NFI internally generates 6 output variables:

1. limit
2. risk score
3. case importance
4. case threshold
5. case grounds
6. decline

[0144] Hereby, the limit directly represents the transaction-individual limit for the current authorization request. This transaction-individual limit is reduced by the risk score as malus ("floating transaction limit").

[0145] The NFI now decides by a simple comparison whether a referral has to be generated or not. A referral is always then generated when the amount requested for authorization is above the transaction-individual limit. By the variables "referral interlock" and "referral_until"-, the NFI decision can be modified.

[0146] The other three variables represent the NFI decision relative to the case generation. The case importance represents to which extent the current authorization request is supposed to be generated as a case. If this value is above the case threshold, than a case will be generated for the authorization. In addition, as the grounds of the decision to generate a case from this authorization message, a text "case class" will be generated describing the kind of suspicion with words. This description is used by the staff members of the Investigation Workflow for being able to carry out a targeted investigation.

[0147] These NFI output variables are transferred directly with the overall information as to the authorization, to the authorization request. The existing authorization software then processes this information further.

[0148] After the computing by the NFI, the NFI transfers the updated time series to the system. The system stores ~~same~~it in the Cardholder File for transferring it again to the NFI upon the next authorization request of this card number.

[0149] The actual decision rules of the NFI are recorded in a file on the authorization computer. Th~~is file is generated by the~~ development tool on the PC generates this file.

[0150] In the following, the decision logic will be explained in more detail. Thereby, the following abbreviations will be used:

Table 1

AvailBal	Amount still available on the card, in Euro
Amount	Amount requested for authorization (in Euro)
BranchCode	Single branch codes
Branch class	Class of the branch to which the VP belongs
CountryCode	Country code from authorization message
CurrencyCode	Currency code from authorization message
GAC	Action code from list definition
ICA_BIN	Origin of transaction
Availment	Still to be defined!
Card age	Age of the card in days, measured in time that has elapsed since "valid as of new"
Card limit	Limit of card in Euro
KI_Range	Association of the card number to ranges that are defined as list
Last answer	How long ago is the last answered Referral/Callme?
Last GAA	Time elapsed since the last GAA withdrawal
Last Referral	How long ago is the last Referral/Callme?
Client	Client identification
Merchant_ID	Merchant ID from list definition
Panic factor	Still to be defined!
POS_Entry	Input kind of authorization request
Terminal_ID	Terminal ID from list definition
Z01	Input variable of counter XXXX
Z02	Input variable of counter XXXX
Z03	Input variable of counter XXXX
Z04	Input variable of counter XXXX
Z05	Input variable of counter XXXX
Z06	Input variable of counter XXXX
Z07	Input variable of counter XXXX
Z08	Input variable of counter XXXX
Z09	Input variable of counter XXXX
Z10	Input variable of counter XXXX
Z11	Input variable of counter XXXX
Z12	Input variable of counter XXXX
Time series length	Number of authorization requests currently stored in time series
Decline	Generation of a "hard" decline
Case class	Declaration which Fraud Supervisory and Fraud Investigation "transfers" so as to depict why exactly this

	case has been generated
Case threshold	This is the possibility to define in FuzzyTECH "variably" a threshold for the case generation
Case importance	Degree to which the current authorization request is being regarded as "caseworthy"
GansLimit	Transaction limit (determined as per user rules (in Euro))
RiskScore	Risk score which is taken as a basis for determining the "malus" in the floating transaction limit
Rule Limit	Transaction limit (determined as per user rules)
Calculate MBF	Calculate Membership Function (fuzzification method)
CoM	Center of Maximum (defuzzification method)
MoM	Means of Maximum (defuzzification method)
Default	Setting of a process variable (visualization interface)
BSUM	Bounded Sum – Operator for calculating the result aggregation
MIN	Minimum Operator (AND-aggregation)
MAX	Maximum Operator (OR-aggregation)
GAMMA	Compensatory Operator for aggregation
PROD	FuzzyOperator for composition
LV	Linguistic variable
MBF	Membership Function
RB	Rule Block

[0151] The system structure describes the data flow in the fuzzy system. Input interfaces fuzzify the input variables. Hereby, the analog values are converted into association levels. The fuzzy interference follows to the fuzzification: With "IF-THEN" instructions fixed in rule blocks, linguistically described output variables are fixed by the input variables. These are transformed in the output interfaces into analog variables by a defuzzification.

[0152] Figure 5 shows the structure for this fuzzy system having input interfaces, rule blocks and output interfaces. The connection lines hereby symbolize the data flow.

[0153] Linguistic variables serve in a fuzzy system for describing the values of continuous variables by linguistic terms. The possible values of a linguistic variable are not digits, but linguistic notions, also called terms.

[0154] For all input, output and intermediate variables of the fuzzy system, linguistic variables are defined. The association function of the terms are uniquely fixed by support points, the so-called definition points.

[0155] The following table lists all linguistic variables together with the term names.

Table 2: Linguistic variables

AvailBal	Low, medium, high
Amount	Low, medium, greater_1000, high
BranchCode	Airport general, store, furs, carpets, sound records, night bars, arms dealer, jeweler, photo, leather, all banking, Hotel general, all 5-type MCCs, massage, automobile general, fun leisure
Branch class	Hotel, airlines, automobile, Buizserv, car_rentals, cashing, clothing, contrctd_services, mail_order, misc_store, non 5311, pers_services, retail, services, transportation, utilities, -cashing
CountryCode	Egypt, Brazil, Ecuador, Hongkong, Indonesia, Israel, Colombia, Malaysia, Marocco, Mexico, Singapur, Thailand, Turkey, Venezuela, Canada
CurrencyCode	F_franc, olden, forinth, olden, i_lira, peseta, pound
GAC	bad_cvc
ICA_BIN	Visa_quer, mexico_special, -mexico_special
Availment	Low, medium, high
Card age	Very_new, new, old
Card limit	Low, medium, high
KI_Range	No_range, fraud_nz, all_others
Last answer	Just_now, v_long_ago
Last GAA	Just_now, medium, long_ago
Last Referral	Just_now, v_long_ago
Client	No_client, gzs, airplus
Merchant_ID	Wempe
Panic factor	Low, medium, high
POS_Entry	Unknown, unknown_o_manually, manually, read, electr_commerce, read_checked
Terminal_ID	Crimin_figaro
Z01	more_than_four
Z02	more_than_four
Z03	more_than_four
Z04	more_than_four
Z05	more_than_four

Z06	more_than_four
Z07	more_than_four
Z08	more_than_four
Z09	more_than_four
Z10	more_than_four
Z11	more_than_four
Z12	more_than_four
Time series length	High
Decline	No_decline, decline
Case class	Counterfeit, hongkong, cvc_queue, hungary, watchlist, jewelers
Case importance	Unsuspicious, medium, suspicious
Limit	_0, _100, _250, _500, _1000, _2500, _7500
RiskScore	Unsuspicious, medium, suspicious
profile	Unsuspicious, medium, risky
Rule limit	_0, _100, _250, _500, _1000, _2500, _7500

[0156] The qualities of the basis variables are listed in the following table.

Table 3: Basis variables

Variable name	min	max	default	Unit
AvailBal	0	20000	0	Euro
Amount	0	20000	0	Euro
BranchCode	0	9999	0	MCC
Branch class	0	32	0	codevalue_list
CountryCode	0	999	0	CC_key
CurrencyCode	0	999	0	CC_key
GAC	0	32	0	codevalue_list
ICA_BIN	0	32	0	codevalue_list
Availment	0	100	0	percent
Card age	0	100	0	days
Card limit	0	20000	0	Euro
KI_Range	0	32	0	codevalue_list
Last answer	0	45	45	days
Last GAA	0	45	0	days
Last Referral	0	45	45	days
Client	0	32	0	codevalue_list
Merchant_ID	0	32	0	codevalue_list
Panic factor	0	100	0	percent
POS_Entry	0	32	0	POS_Entry_Mode

Terminal_ID	0	32	0	codevalue_list
Z01	0	32	0	number
Z02	0	32	0	number
Z03	0	32	0	number
Z04	0	32	0	number
Z05	0	32	0	number
Z06	0	32	0	number
Z07	0	32	0	number
Z08	0	32	0	number
Z09	0	32	0	number
Z10	0	32	0	number
Z11	0	32	0	number
Z12	0	32	0	number
Time series length	0	32	0	AuthoriRequests
Decline	0	1	0	-
Case class	0	32	0	codevalue_list
Case threshold	0	1000	750	threshold
Case importance	0	1000	0	per mil
Limit	0	30000	0	Euro
RiskScore	0	1000	0	per mil

[0157] The default value is adopted by the output variable, when no rule fires for this variable. Various methods can be used for the defuzzification, which either furnish the "most plausible result" or the "best" compromise.

[0158] To the compromise-forming methods belong:

CoM (Center of Maximum)

CoA (Center of Area)

CoA BSUM, a variant for efficient VLSI implementations

[0159] The "most plausible result" is furnished by:

MoM (Mean of Maximum)

MoM BSUM, a variant for efficient VLSI implementations

[0160] The following table lists all variables linked with one interface, as well as the corresponding fuzzification or defuzzification method.

Table 4: Interfaces

Variable name	Type	Fuzzification/defuzzification
AvailBal	Input	calculate MBF
Amount	Input	calculate MBF
BranchCode	Input	calculate MBF
Branch class	Input	calculate MBF
CountryCode	Input	calculate MBF
CurrencyCode	Input	calculate MBF
GAC	Input	calculate MBF
ICA_BIN	Input	calculate MBF
Availment	Input	calculate MBF
Card age	Input	calculate MBF
Card limit	Input	calculate MBF
KI_Range	Input	calculate MBF
Last answer	Input	calculate MBF
Last GAA	Input	calculate MBF
Last Referral	Input	calculate MBF
Client	Input	calculate MBF
Merchant_ID	Input	calculate MBF
Panic factor	Input	calculate MBF
POS_Entry	Input	calculate MBF
Terminal_ID	Input	calculate MBF
Z01	Input	calculate MBF
Z02	Input	calculate MBF
Z03	Input	calculate MBF
Z04	Input	calculate MBF
Z05	Input	calculate MBF
Z06	Input	calculate MBF
Z07	Input	calculate MBF
Z08	Input	calculate MBF
Z09	Input	calculate MBF
Z10	Input	calculate MBF
Z11	Input	calculate MBF
Z12	Input	calculate MBF
Time series length	Input	calculate MBF
Decline	Output	MoM
Case class	Output	MoM
Case threshold	Output	default
Case importance	Output	CoM

Limit	Output	MoM
RiskScore	Output	CoM

[0161] Rule blocks

[0162] The controller behavior in the various process situations is fixed by the rule blocks. Each single rule block contains rules for a fixed set of input and output variables.

[0163] The "IF" part of the rules thereby describes the situation in which the rule is supposed to be valid; the "THEN" part describes the reaction thereto. By the "Degree of Support" (DoS), the single rules can be imparted a varying weighting.

[0164] For evaluating the rules, the "IF" part is first calculated. Hereby, various methods can be used, which are fixed by the operator type of the rule block. The operator can be of the MIN-MAX, MIN-AVG or GAMMA type. The operator behavior is in addition influenced by a parametrization.

[0165] For example:

MIN-MAX having the parameter value 0 = Minimum-Operator (MIN).
MIN-MAX having the parameter value 1 = Maximum-Operator (MAX).
GAMMA, having the parameter value 0 = Product-Operator (PROD).

[0166] The Minimum-Operator is the generalization of the Boolean "AND", and the Maximum-Operator is the generalization of the Boolean "OR".

[0167] The results of the single rules are summarized in the subsequent fuzzy composition to overall conclusions. The BSUM method hereby considers all rules firing for one condition, whereas the MAX method takes only dominant rules into account.

MARKED UP VERSION OF SUBSTITUTE SPECIFICATION

~~CLAIMS~~

What is claimed is:

1. A method which is implemented on a computer and which is provided for identifying and determining fraudulent transaction data in a computer-controlled transaction processing system comprising a prediction model for receiving current transaction data, for processing the current transaction data, and for outputting at least one output value that depicts a probability of a fraudulent transaction, wherein, on the basis of stored data, for

- a time series analysis of earlier transactions with respect to the same means of payment or user, and
- expert rules concerning parameters which occur in a statistically significant cumulative manner during fraudulent transactions, especially with respect to the origin of the means of payment/user, to the branch and to the beneficiary of the transaction, as well as to the magnitude or value of the transaction, the evaluation is carried out by means of the prediction model with respect to the risk of the current transaction being fraudulent, and a corresponding output value is generated,

wherein the prediction model combines a limit, which is essentially based on the expert rules and which is specific for the type of transaction, with a value, which is essentially based on the time series analysis and which is specific for the current transaction, in order to generate the output value,

the combination being carried out in a floating manner so that output values can be generated which vary according to the extent of the suspicion of misuse and which can be used to initiate different reactions to the current transaction request.

2. The method according to claim 1, wherein the time series analysis is implemented in the form of fuzzy logic rules.

3. The method according to claim 1 or 2, wherein the expert rules are implemented in the form of fuzzy logic rules.

MARKED UP VERSION OF SUBSTITUTE SPECIFICATION

~~Abstract~~

ABSTRACT OF THE DISCLOSURE

~~The invention relates to a method which is implemented on a computer and which is provided~~A method and system for identifying and determining fraudulent transaction data in a computer controlled transaction processing system ~~comprising~~using a prediction~~model for receiving current transaction data, for processing the current transaction data, and for outputting at least one output value that depicts a probability of a fraudulent transaction. According to the invention, the~~model. The prediction model is used to carry out the evaluation with regard to the risk that the current transaction is fraudulent, and a corresponding output value is generated. This evaluation is carried out using stored data of a time series analysis of earlier transactions~~with respect to the same means of payment or user~~ and to expert rules concerning parameters which occur in a statistically significant cumulative manner during fraudulent~~transactions, especially with respect to the origin of the means of payment/user, to the branch and to the beneficiary of the transaction, as well as to the magnitude or value of the transaction.~~transactions. The prediction model combines a limit~~, which is essentially based on the expert rules and which is specific for the type of transaction,~~ with a~~value, which is essentially based on the time series analysis and which is specific for the current transaction,~~value in order to generate the output value. The combination is carried out in a floating ~~manner so that output values can be generated which vary according to the extent of the suspicion of misuse and which can be used to initiate different reactions to the current transaction request~~manner.

EXPERT SYSTEM

FIELD OF THE INVENTION

[0001] The present invention relates to the detection of the fraudulent use of customer accounts and account numbers, including, for example, transactions with credit cards. The present invention in particular relates to an automated fraud detection system and a method using a prediction model for the pattern recognition and classification so as to pick out transactions having a high likelihood of fraud. In the following discussion, the term "credit card" will be used for descriptiveness purposes; the here discussed methods and fundamentals, however, apply as well to other kinds of electronic payment systems, such as, for example, customer credit cards, automated machine-readable cash cards and telephone cards.

BACKGROUND INFORMATION

[0002] The establishments issuing credit cards have at all times tried to restrict their losses caused by fraud in that the fraudulent use of the card is indicated before the card holder has notified a lost or stolen card.

[0003] An effective model for the fraud detection was supposed to result in high catch rates at a low impediment of legal transactions in the real time operation. It was supposed to be able to adapt to changing fraud methods and patterns, and was supposed to have an integrated learning capacity supporting this capacity of adaptation.

[0004] The WO-A-8 906 398 is believed to describe an element for the analysis of a transaction by means of data processing: in that only that data is extracted, which may be useful for the analysis of the transaction; in that signals are cancelled corresponding to a transaction which is presumed to match with a set of predetermined rules; in that it is filtered so as to eliminate non-significant modifications of the transaction to be analyzed; and in that signals are classified into one or several classes according to a predetermined criterion. It is believed that this element is suited for the application of issuing payment authorizations to credit card users.

[0005] A further reference, EP-A-0 418 144, is believed to describe a method for restricting the risks associated with a computer-assisted transaction, in that the transaction request may be compared to predetermined statistical data, which seems to be representative of a risk score of a non-conform use. The statistical data describes the mean number or the quantity of transactions performed during the sequence of successive periods of time, and is derived in that the time is divided into successive, non-equal periods, the duration of which are selected in a manner that the likelihood of a performed transaction or the mean amount for each single period of time are substantially equal.

[0006] The EP-0 669 032 is believed to describe fraud detection method implemented on a computer, and a corresponding hardware, which includes means for prediction models. Current transaction data is received and processed, which then results in a plurality of output values containing a hit value representing the likelihood for a fraudulent transaction.

[0007] It is believed that this method requires several steps, which have to be carried out prior to the processing steps for the current data, namely:

a. generating a user profile for each individual of a plurality of users out of an enormous number of variables relative to previous transactions, and of personal user data containing for each user values out of a plurality of user variables, each user profile defining a pattern for the transaction history of a user;

b. deriving variables concerning proven previous fraud in that data of previous transactions are preprocessed, these values containing a plurality of previous transactions for a plurality of transaction variables;

c. training of means for prediction models with said user profiles and said variables concerning previous fraud, so as to obtain a prediction model; and

d. storing said obtained prediction model in the computer.

[0008] Then, the processing of the current data is carried out in that

e. the current transaction data for a current transaction of a user is received;

f. the user data concerning the user, is received;

g. the user profile associated with the user, is received;

h. the obtained current transaction data, user data and the user profile are preprocessed so as to derive variables relative to a current fraud for the current transaction;

i. the likelihood of fraud in the current transaction is determined in that the prediction model is applied to the current fraud-related variables; and

j. an output signal is emitted from the means for the prediction model, which signal indicates the likelihood of fraud for the current transaction.

[0009] This system supports on a neuronal network for training the means for the prediction model. Said training is supposed to mainly change the means for the prediction model so as to keep the prevention of legal transactions low, and to improve the performance of the system for the detection of fraud.

[0010] Hereby, the system supports on a set of fixed (yet variable) values representing various aspects of the transaction. These values are differently weighted in processing, and one important function of the training based on the neuronal network, is the variation of said weighting, basically resulting in a "learning" capacity for this system. Such neuronal networks represent a linking of "neurons" in the meaning of simple mathematical transfer functions. For generating a "learning capacity" here, a corresponding algorithm is used – e.g. according to EP 0 669 032, for adapting the "weights" with the data rating in the neuronal network.

[0011] In spite of all that, the system for combining the different parameters and data, employs usual logic algorithms and functional relationships for obtaining the hit value. For each current transaction, it carries out a calculation based on conventional logic, views the results (later), and varies, if necessary, the algorithm.

SUMMARY OF THE INVENTION

[0012] An object of an exemplary embodiment and/or exemplary method of the present invention is to create an automated system which uses the available information, e.g. on the card holder, merchants and shops for monitoring transactions and picking out these which are probably fraudulent, and which is able of thereby discovering a relatively higher portion of cases of frauds at a relatively lower prevention of legal transactions. A further object of an exemplary embodiment and/or exemplary method of the present invention is to provide a system that should preferably also be capable of dealing in a fast real time operation with a large number of variables independent of each other, and should feature the capacity of redeveloping the basic system model as new patterns for upcoming fraud behavior.

[0013] It is believed that these objects may be achieved with a method for use in a computer controlled transaction system for determining an extent of a risk of a current transaction in the computer controlled transaction system being fraudulent according to claim 4, a system for determining an extent of a risk of a current transaction in a computer controlled transaction system being fraudulent according to claim 10 and a computer-implemented method for identifying and determining fraudulent transaction data according to the features of claim 16.

[0014] Reference is made to the complete scope to EP 0 669 032 which is hereby incorporated by reference.

[0015] As can be seen from the following description where an exemplary embodiment of the present invention is described with reference to the method of the EP 0 669 032 to emphasize the difference of this exemplary embodiment of the present invention and this

method, there exist major differences between this exemplary embodiment of the present invention and the method of the EP 0 669 032, residing, e.g. in the basic approach and in the corresponding basic structure, as well as in various details of the data generation and processing.

[0016] It is believed that an essential difference results from the fact that according to an aspect of this exemplary embodiment of the present invention there is no use of a user profile as a part of the prediction model. Instead, this exemplary embodiment of the present invention works with a combination of expert rules, for one, and an analysis of preceding operations of using the payment means, for another, which is used for the transaction to be currently evaluated.

[0017] According to another aspect of an exemplary embodiment of the present invention, the expert rules concern a selection of typical elements of an individual transaction based on experience values, i.e. the analysis of past cases of misuse, which elements are indicative for an increased risk of misuse. According to yet another aspect of an exemplary embodiment of the present invention, the origin of the payment means is in particular relevant (e.g. the card), the branch and the person beneficiary of the payment to be authorized, and the payment amount.

[0018] According to yet another aspect of an exemplary embodiment of the present invention, the analysis of preceding events of use of the same payment means preferably comprises the latest events, for example, the last five to twenty transactions (this could, however, also go further back).

[0019] In contrast to the method of the EP 0 669 032, according to yet another aspect of an exemplary embodiment of the present invention, there is no use of a conventional neuronal network in combination with a learning algorithm.

[0020] The method and system according to exemplary embodiments of the present invention use fuzzy logic for determining whether a certain transaction has to be considered as being fraudulent.

[0021] In the decision system preferred according to yet another aspect of an exemplary embodiment of the present invention, the expert rules, as well as the rules functionally corresponding to the prior art neuronal network, may be memorized for the descriptive statistics as fuzzy rules, and therewith do not differ in the calculation method, but in the gaining method.

[0022] The expert knowledge may directly be formulated as fuzzy rules. These define a limit for each transaction type that corresponds to the (user-specific) "risk readiness".

[0023] The information from the use history of the payment means may be likewise transformed into fuzzy rules by means of a "NeuroFuzzy module". The NeuroFuzzy module may use a modification of that training algorithm, which may also be used in most neuronal networks, namely the Error Backpropagation algorithm described in the literature. Since in this way the information from past data (hence that, what is, for example, memorized in the weights of the trained neuronal network according to EP 0 669 032) is available as readable and interpretable/modifiable fuzzy rules, this information can be completed, verified and extended in any manner. With respect to the input and output data, the "neuronally" generated fuzzy rules can use the same variables as the expert rules.

[0024] The "neuronally" generated fuzzy rules according to yet another aspect of an exemplary embodiment of the present invention, are preferably based on an analysis of preceding transactions with respect to such factors as the average transaction amount, the portion of cash disbursements, the portion of foreign jobs, of travel cost use, the previous occurrence of suspicious cases, etc., and with respect to "dynamic" criteria such as, for example, the current exhaustion of the limit of the credit card concerned. The result of this analysis is also designated as "time series". This rule system thus assesses a dynamic risk for each transaction in the form of a "bonus" or a "malus".

[0025] Thus, it is believed that the invention permits the merging of statistical models with expert knowledge. Instead of simply calculating for each event, as it is the case with the above-mentioned references, a fraud probability, the limit defined for each transaction type, is floatingly combined with the dynamic risk ("bonus" or "malus") of the specific current transaction to a (floating) transaction limit.

[0026] It is believed that this enables various differentiated treatments of "eye-catching" transactions, e.g. the immediate interlock, or instead, the remittance for an individual check, e.g. through a person in charge.

[0027] In the above-mentioned references, a transaction lying above the risk threshold normally is stopped. Basically, according to these references, there is only the release or interlock as a result of the check. The method system according to yet another aspect of an exemplary embodiment of the present invention instead enables gradual reactions; for example, a suspicious case can be generated (and therewith enter into the "time series" for this credit card, which will be referred to for future transactions), although the current transaction is being authorized. In case of a stronger suspicion, a re-check (referral) of the current transaction would be initiated (prior to the possible authorization thereof); with a still stronger suspicion, the transaction would be rejected (decline).

[0028] Substantial differences between the above references and a method/system according to an exemplary embodiment of the present invention result with respect to the model formation, hence, the generation and recognition of misuse patterns (fraud patterns).

[0029] It is believed that the above references are based on a "passive data gain". In other words, exclusively already present past data is referred to for the model formation. This means that, for being able to recognize a fraud pattern in the model at all, (a) a sufficiently long time must have elapsed, so that the fraud messages have already come back (in most cases only after the customers have read their statement of accounts), (b) enough cases for a secure training must be given (a neuronal network functions only in this case / there exist

fraud cases which are very rare but cause a high individual damage, and which are only very difficult to cover in the model, (c) an immunization of the authorization operation is only possible at all after laborious manual retraining.

[0030] The data gain according to yet another aspect of an exemplary embodiment of the present invention, however, is "active". If the first suspicious factors of a new fraud pattern arise, then new rules will be defined immediately initiating an investigation of exactly these cases by actively contacting the customers. Thus, many secured data will be available within a few hours in the ideal case as to whether a new fraud pattern has actually arisen, and how it differentiates from other patterns. This analysis (it makes no difference by means of which method) namely can only then be carried out when enough secured data is present.

[0031] It is believed that the methods of the model establishment in accordance with a reference mentioned above leads to the fact that the experience of human analysts cannot sufficiently be used, and expectations as to future fraud patterns cannot gain entry. In these methods, the neuronal network virtually constitutes a "black box" of fixed, rigid criteria, which still are only modified "automatically" with respect to their "weights", hence, as the result of algorithms in turn fixed beforehand. As far as expert rules are used at all together with neuronal networks, neuronal network and expert rules run independently side-by-side. Through the NeuroFuzzy approach according to yet another aspect of an exemplary embodiment of the present invention, the predictive model trained with data, is no longer a black box, but is generated in the form of fuzzy rules. These can be directly interpreted and modified by experts.

[0032] The floating transaction limits according to yet another aspect of an exemplary embodiment of the present invention permit an efficient combination of "hard facts" and "soft facts". It is believed that this enables the "soft" and "hard" facts to be modeled in a consistent and cooperative way. With the "black box" approach of the above references, this is of no importance, since there, no knowledge-based modeling takes place. With the invention which enables and preferably also provides that an automatic model formation and human expertise are combined in the running operation, this is very relevant.

[0033] The invention will be explained in more detail in the following by means of an exemplary embodiment comprising configurations of the inventive basic principle particularly preferred at present.

BRIEF DESCRIPTION OF THE DRAWINGS

[0034] Figure 1 shows an exemplary embodiment of a principal information exchange performed in an exemplary embodiment of the method and system of the present invention.

Figure 2 shows an exemplary embodiment a data flow with presumed or recognized misuse cases occurring in an exemplary embodiment of the method and system of the present invention.

Figure 3 shows another exemplary embodiment a data flow occurring in an exemplary embodiment of the method and system of the present invention.

Figure 4 shows yet another exemplary embodiment a data flow occurring in an exemplary embodiment of the method and system of the present invention.

Figure 5 shows an exemplary embodiment of a structure for this fuzzy system having input interfaces, rule blocks and output interfaces in an exemplary embodiment of the method and system of the present invention.

DETAILED DESCRIPTION

[0035] An exemplary embodiment of the present invention relates to an authorization system for credit card transactions, and therewith to a basic constellation similar to that of the initially discussed references. From an existing network comprising points of use for the credit cards usable in the system, come authorization requests which have to be handled and answered in real time.

[0036] The handling of the authorization requests takes place in the inventively configured authorization system schematically shown in the Figures 1 through 4.

[0037] In the exemplary embodiment, the system comprises several computers but can of course also be realized on a central computer or by means of a computer network.

[0038] In the exemplary embodiment, the system comprises a "tandem" computer with a database A, an "SGI" server (SQL server) with a database B, and a "host system" with a database C.

[0039] On the tandem computer, a software may be implemented serving for data transfer, data reprocessing (criteria derivation), time series calculations and time series updates, etc., as will become clear later. Moreover, the inventive decision logic is implemented on the tandem computer, including fuzzy expert rules and NeuroFuzzy models, and making the decision on authorization requests. The software implemented on the tandem computer in summary will be designated "NeuroFuzzy Interference Machine" (NFI) in the following.

[0040] The SGI server, if the case may be in conjunction with a corresponding number of PC clients, serves in particular for the implementation of the software for the "Investigation Workflow" (IW) for the follow-up on cases of suspicion, and for the "Online Data Mining Module" (ODMM), as will be explained later.

[0041] The host system contains and receives the essential historic and current data as to payment means and user, required for the treatment of the authorization requests.

[0042] Figure 1 shows an exemplary embodiment of a principal information exchange performed in an exemplary embodiment of the method and system of the present invention as follows: The authorization system obtains data (1) for a cardholder file from database [C] of the host system. With a modification of the data of the cardholder file, only the data of a card number relevant for the authorization is transferred to the authorization system. Events such

as card interlocks having a high priority, are immediately transferred, others having a low priority, are transferred only much later. The data transfer (update) may take place hourly.

[0043] The SGI server receives (2), via the existing network, the authorization requests from the authorization tandem computer provided with the NFI-initiated action (same is comprised of: case importance, case class, case threshold, referral decision, risk score, limit and action code), as well as the current time series information. (The real time requests necessary for this purpose are in the range of minutes. The overall information as to an authorization request is compressed to a message by the NFI, which message is then transferred to the SGI server).

[0044] The SGI server further receives from the host system any posting information, misuse information and, if the case may be, cardholder main data, which cannot be extracted from the cardholder file (3). The database of the SGI server [B] stores this data as long as required, depending on the storage expansion. The SGI server lodges the server component, be it of the Supervisory Workflow (ODMM) or also of the Investigation Workflow (IW).

[0045] Figure 2 shows an exemplary embodiment of the data flow with presumed or recognized misuse cases.

[0046] The Investigation Workflow (IW) (6) serves for the treatment, in particular by means of staff members (Call Center), of recognized and presumed fraud cases.

[0047] In the Call Center, it is ascertained whether the presumed cases of misuse actually are cases of misuse. A corresponding information (7) to the SGI server takes place.

[0048] Apart from this main task, the SGI server fulfils still another main task:

[0049] The SGI server database stores the data necessary for the discovery of new fraud patterns, and processes it for an analysis by the Online Data Mining Module (ODMM). For this purpose, the misuse-relevant data is buffered in database [B]. In the Fraud Supervisory

Center, new fraud rules are then defined by means of this information (4), and the existing fraud rules are continuously checked for their efficiency.

[0050] The correspondingly modified fraud rules in the form of a file are then transferred from the Fraud Supervisory Center to the authorization computer (5). For doing this, the file is brought to the SGI server from the PC. On the SGI server, an automatic job is installed which recognizes when the time stamp of the file has changed, and performs an exchange of said file on the tandem in this case and also communicates to the NFI that has to read-in this file anew.

[0051] Hence, two workflows result *in toto* as may be taken from Figure 4:

1. The Supervisory Workflow ODMM adapts continuously the decision strategy of the prevention system to the changing misuse patterns.

2. The Investigation Workflow IW checks the decisions of the prevention system by individually treating the reported and presumed cases of misuse.

[0052] Both Workflows are indirectly connected via the (mean) operative EDP level. If the decision strategy is modified in the Supervisory Workflow, then other referrals will be generated by the prevention system, which will be investigated in the Investigation Workflow.

[0053] A misuse not timely recognized by the prevention system, as well as an erroneous misuse presumption, is verified by the Investigation Workflow and stored in the database of the SGI server. Hereto accesses the Online Data Mining Module (ODMM) and proposes a corresponding modification of the decision strategy to the fraud experts in the Fraud Supervisory Center.

[0054] The overall calculation, hence the flow of the fuzzy interference through the rule work, as well as the entire profile formation and initialization, is taken over by the NFI itself; an external control is not required. The interface contains further functions for the initialization and configuration of the decision logic (these functions have to be invoked once

upon loading of the prevention module), which, however, have not to be invoked per authorization request.

[0055] The SQL database of the authorization computer (Cardholder File) is supplemented by a field "time series". This field stores the last authorization requests to this card number (profile of use) in a compressed form. When an authorization request enters the system, the complete data set of the card is loaded from the database. Here, the binary object "time series" has in addition to be loaded from the database and transferred to the NFI. The binary object profile of card use is then generated in an extremely compressed form, so that is can be efficiently stored in the SQL database for the real time access. Additional computing time by the read-out and re-storage of the card profile upon each authorization request will not cause a noticeable computing effort, since the data set of a card is in any case read out upon each authorization request. After the decision, the NFI updates the time series by the authorization just received. Exactly as the limits updated by the authorization, the updated time series has to be written back into the database, as well.

[0056] Furthermore, the Cardholder File is supplemented by two date fields, in each case one for "no referral until" (this field is set upon a positively answered referral for ensuring that, immediately after a positive ID, the card holder directly receives again a referral on the occasion of the next transaction), and one for "short referral until" (upon an acute suspicion, this date is set so as to forcibly generate a referral with each authorization request up to this date). These fields are set or reset through the authorization system. The data is delivered to the NFI by the authorization system, the NFI evaluates the data and decides whether a referral or decline or, if the case may be, a case shall be generated. Since the NFI, if the case may be, also contains client-dependent rules, the NFI has to recognize the client from the card number. (A client is, for example, the client of the processing company, for whom the fraud processing is carried out).

[0057] The development component is part of the Supervisory Workflow and a graphical development and analysis software, which is installed on Windows/NT workstations (clients).

Hereby, existing computers can be concerned which are also used for other tasks, or a separate computer can be provided.

[0058] Proceeding from the development software, the developer may modify the fuzzy decision system of the tandem. Hereby, the ongoing authorization process is in any case neither stopped, nor disturbed nor decelerated.

[0059] If new fraud patterns become known, then the development component allows to take same into consideration by modification of known and definition of new rules. Thereby, these new rules and modified rules are transferred to the NFI, where the new rules have an instantaneous effect on the authorization behavior.

[0060] All authorization requests are handed over by the tandem to the SGI server via TCP/IP. The SGI server establishes a new record for each authorization request, and fills the same with all necessary information.

[0061] If the case importance of an authorization request is above the case threshold, then the SGI server establishes a case in addition. A case is comprised of an entry in the case table and the associated sub-tables.

[0062] In summary:

[0063] Each message incoming from the tandem describes an authorization request.

[0064] A record is established for each authorization request.

[0065] The case generation is independent of the referrals, i.e., a case may be generated without a referral having been generated, and a referral may be generated without a case being generated.

[0066] This interface is installed on part of the SGI servers. Likewise is the generation of the corresponding entries in the SGI server tables.

[0067] The Investigation Workflow serves for following up the possible fraud cases and referrals. Hereby, the case importance ascertained by the NFI is taken as a basis for the case grading. Whether a referral has been generated for this authorization request or not, is not important for the generation of a case. The case generation works with its own decision logic, which can also contain rules deviating from the fraud rules. Prevention strategies can hereby be tested so to speak, as a "dry run". Therewith, also such cases can be followed up in the Investigation Workflow, in which the suspicion did not suffice for a referral generation.

[0068] Compressed storage of the authorization history ("time series")

[0069] The NFI works with neuronal models which are based on the analysis of previous transactions.

[0070] The problem of such an analysis is that during the treatment of an authorization request, a polling and analysis of past transactions is not possible in real time. Therefore, the NFI has to store a brief history temporarily in a ring buffer. (A ring buffer is a storage having a fixed number of places switched in series. Each newly stored object is pushed into the ring buffer "at the front", thus advancing all objects already present in the ring buffer in each case by one position. The object in the last place thereby completely falls out of the ring buffer.) It is of particular importance here that the time series requires as little storage place as possible (each byte per card results in a net storage place requirement of about 7 megabyte in the database of the authorization computer), and that it is allowed to be read and written as fast and efficiently as possible.

[0071] The time series formation is for this reason based on an algorithm, which generates and updates said ring buffer in such a manner that it is efficient to store and compute. For the storage, a compressed memorization in the converted integer format is used.

[0072] The time series information thereby represents, for example, a condensed history of the last 15 authorization requests, which enables a calculation of dynamic criteria (exhaustion, panic, gas station use, etc.) The time series information in addition permits the assessment of aggregated variables such as: average shopping amount, cashing portion, foreign country portion, travel cost use portion, when has a referral been issued for the last time, and when has a referral been answered for the last time.

[0073] Since the time series information has to be stored (in the ring buffer for each authorization request) 15 times, a compression of the information is particularly important.

[0074] Since the profile is stored in the database as binary object (string format), the individual partial information of each transaction can be coded in the ring buffer as integers of an arbitrary bit length. However, a reasonable division of individual bit lengths to the bytes of the string format has been chosen for keeping the calculation and update of the profiles from becoming computationally not too laborious. Hereby, the shortest possible storage form "exact bit" is not always chosen, rather there results a compromise of storage place requirement minimization and computational performance maximization.

[0075] As to the stored fields in detail:

[0076] Date

[0077] The storage of the date in the minute format enables the simple calculation of time differences in integer arithmetic of a 16-bit digit (with a 16-bit-minute resolution, a maximum of 45 days can be represented, which is sufficient for the calculation of time differences in the profile).

[0078] The 16-bit values resulting with the subtraction of such minute values for the time differences are directly used as input variables of the NFI without any expansive computationally scaling modifications.

[0079] With the maximum storage length of the minute date after a deadline of 24 bits, however, a reset of the profile information has to ensue every 31 years.

[0080] If this entry "date" is equal to "0", then this means that said entry is not yet used in the ring buffer.

[0081] Amount

[0082] Has to be divided by 10 so as to result in the Euro amount. Hereby results an optimized utilization of the 20-bit digit range.

[0083] Deviations in the amount of below Euro 0.10 are unimportant for the misuse prevention, and the maximally representable amount of over Euro 100,000.00 is also sufficient. Requested values of over Euro 100,000.00 are cut down in the ring buffer to Euro 100,000.00.

[0084] MCC

[0085] Contains the branch code of the contractual partner who has requested the authorization.

[0086] ICA

[0087] Describes all issues by means of their ICA numbers.

[0088] Country code

[0089] For the time series inspections, the country code is sufficient for the origin determination. Same is maximally three-digit, therefore 10 bits are sufficient for the representation (according to MC Quick Reference Booklet, October 97).

[0090] POS

[0091] Receives the 5 possible POS Entry modes. 3 bits, it is true, would suffice so as to depict said 5 possible POS Entry Modes, the representation in 4 bits, however, offers arithmetic advantages.

[0092] Status

[0093] Status describes, for example, whether the expiration date was wrong, or whether a CVC problem has arisen, etc. (On the magnetic card, the card number is extended by a three-digit code (CVC-1). This three-digit code is not calculable. Therewith, a quite good identification of a genuine card is possible by means of this examination.) It is hereby guaranteed that non-authorized requests can be taken into consideration in the profile.

[0094] Fraud Supervisory Workflow

[0095] The Fraud Supervisory Workflow includes all tools which are used for controlling the decision logic and for waiting. In detail, these are the modules:

[0096] Online Data Mining Module

[0097] For the systematic recognition of new misuse patterns, as well as for the continuous check of the hit security of currently defined decision rules.

[0098] Decision logic

[0099] In this module, the decision components are developed, monitored and controlled.

[0100] Analysis NFI

[0101] The analysis NFI serves for testing new decision logics on past scenarios.

[0102] Online Data Mining Module (ODMM)

[0103] The Online Data Mining Module is comprised of a server component on the SQL server, as well as of a client component on a PC. The client component cooperates with the server via Pass-Through Queries and linked tables.

[0104] The ODMM works with tables in which the authorization requests and cases necessary for the analysis are recorded.

[0105] The ODMM Client contains the following information as to each transaction:

[0106] card number (together with the date and time of the transaction, this information serves for the unique allocation of each transaction (key). Since several events (e.g. several authorization requests, misuse messages, answered referrals, etc.) may belong to a transaction, which can take place at different times, the earliest date will always be used here. This corresponds to the logic that the events belonging to this transaction all refer to the first payment request, which has become known in the system.

[0107] Date and time of the transaction

[0108] Amount in Euro

[0109] Type of transaction (authorized or non-authorized transaction; with non-authorized transactions, for example, no authorization request exists, a posting and a misuse message, however, can be present)

[0110] Misuse (has misuse occurred?)

[0111] Referral (has a referral been generated, if yes, how was it answered)

[0112] Information from the authorization request or the posting (branch code, Country Code origin, POS Entry)

[0113] Random number (selection of a sampling quantity)

[0114] The tables supplying this information are polled by the ODMM Clients via Pass Through Queries.

[0115] The server allocates posterior incoming misuse messages to transactions already entered in the TRX table. The results are likewise updated for the statistic component.

[0116] Systematic search

[0117] The systematic search runs on the server as Pass-Through Query and generates a table comprising rules which are currently not activated, and which would be reasonable to be included. A misuse amount is allocated to each rule, which could have been prevented during the examination period if this rule had been active. For verifying this statement, each rule also contains the ratio of erroneously versus legitimately refused authorization requests (F/P rate), the number of illegitimate referrals, which enable the judgment as to adoption or refusal of the rule. It is possible to filter the rules in advance by indicating a determined misuse amount and F/P rate. With smaller amounts or higher F/P rates, the found rules are blinded out. The weighting between the misuse amount and the F/P rate can be set during the classification. Therewith, it can be fixed anew with each systematic search, of which importance each of the two variables is supposed to be for the examination.

[0118] Rule optimization

[0119] The negatively answered referrals which could not confirm a misuse, serve for the recommendation to deactivate rules as a basis. If a referral is answered negative, then the associated data set will no longer flow into the analysis as a misuse, but as a good transaction. If it turned out then that the rule has not prevented enough misuse and has prevented many

good transactions, then it will be proposed to be deactivated. In this analysis, too, the weighting between the misuse amount and the F/P rate can be set. Therewith, it can be fixed anew with each systematic search, of which importance each of the two variables is supposed to be for the examination.

[0120] Decision logic

[0121] The access to the decision logic ensues over the Fraud Supervisory Workflow:

[0122] The block "Fraud Supervisory Workflow" represents the PC networks in the staff SI. These administer decision logics of an arbitrary number, be it for the filing or as intermediate development stages. (The actual data for the decision logics are centrally stored on the SGI server, so that all fraud analysts have access to same. The access to these decision logics takes place by the PCs with the help of the "Fraud Supervisory Workflow" software.) Each of the decision logics is comprised of the three components, lists, time series and rules. By pressing the respective keys, the corresponding editors for the components will open.

[0123] In the productive operation the decision logic "Operation" always runs. By pressing the key [transfer], the decision logic "Operation" currently developed in the PC, is transferred to the tandems, and is activated.

[0124] The two decision logics for the analysis of scenarios run on the SGI server. By pressing the key [transfer], the decision logic "Test" currently developed in the PC, is transferred to the SGI servers, and is activated.

[0125] Proceeding during the development

[0126] The basic proceeding during the development of decision logics is the following. The decision logic "Operation" runs on the authorization computer. By pressing the key [transfer], the decision logic "Test" will be overwritten with the decision logic "Operation". (Hereby, not a physical overwriting from the tandem to the SGI server is

concerned. The SGI servers also dispose of a copy of the decision logic, whereby the overwriting is directly carried out on the SGI servers.)

[0127] The decision logic "Test" can hereby be modified on the PC, and with the assistance of the analysis NFI, the test of modifications takes place by a direct comparison of the "Test" system and the "Operation" system.

[0128] If the modifications carried out on the decision logic "Test" are successful, then the decision logic "Test" will be overwritten with the decision logic "Operation" by pressing the key [transfer]. After the new decision logic has become operational, the proceeding starts anew.

[0129] Each new transaction is provided with a judgment of case worthiness by the NFI machine. An auxiliary module marks a transaction as a case, when said transaction fulfils a case criterion (MCC, ICA, CNT, POS, amount class, case worthiness).

[0130] Optionally, it can be determined how far the history of the transaction and the posting of an event reach back. A period of 4 – 6 weeks is considered to be reasonable.

[0131] If a transaction belongs to a category of all possible cases, then a new record will be established in the Investigation Workflow-inherent table. This record contains the following single data:

- card number
- transaction data (date/hour, MCC, CNT, ICA, POS, amount)
- case status (is the case new or has it been closed)
- case importance (the case importance FW represents the NFI score)
- case class (the case class indicates why a transaction has become a follow-up case or to which category the transaction belongs. The identification consequently includes indications as to MCC, ICA, CNT, POS, amount class, FW.)
- user name

- date of resubmission
- close status (the close status of a case supplies details on the result of the treatment after closing the case, and may contain the following information: "no fraud", or "no fraud estimated", "fraud confirmation impossible" or "fraud estimated".)

[0132] The card number is the link (pointer) to the past transactions with the same card number on the DBMS of the SGI server. Together with the card number main data, all data are complete for the Fraud Investigation Workflow.

[0133] NFI input variables

[0134] The NFI is integrated into the authorization process over a token protocol. From here, the NFI takes out all input variables, as well as the time series as binary data object (string).

[0135] As a special form of authorizations, the NFI has to interpret the messages on a referral interlock or a referral_until.

[0136] Referral_until: the parameter referral_until (short referral) is used with a misuse suspicion for preventing authorizations. It is manually activated by an authorization.

[0137] The NFI memorizes the referral_until date in the card profile, and checks during the authorization whether the transaction date is smaller than the referral_until date. If this is the case, a referral will always be generated by the NFI.

[0138] The referral_until parameter is transferred for analysis and reconstruction to the SGI computer via the TCP/IP interface as a component of the transaction data set.

[0139] Referral interlock: the referral interlock is used for preventing the further initiation of referrals after a positive identification or after viewing the past transactions. The referral interlock can adopt the conditions "valid" or "not valid". If it is "valid", then a

previously set parameter is activated indicating a fixed offset from the current transaction date (e.g., transaction date + 3 days). The referral interlock is always given in the form of a date, until which it shall last. It namely can only be determined at the current moment whether the interlock therewith is valid or not.

[0140] The referral interlock can be activated, for one, proceeding from the Investigation Workflow. For another, the referral interlock can also be indirectly initiated by the authorization service, when a positive identity check has taken place after a referral. After a positive identity check, the authorization service initiates a transaction, which is processed in the NFI. The NFI writes the current referral interlock into the Cardholder File on the authorization computer.

[0141] The case has to be avoided of a referral interlock, as well as the referral_until date both being valid. For this reason, when one value is set (e.g. referral_until), the respective other value is erased (e.g. referral interlock).

[0142] Internal output variables

[0143] If all input variables are present, which are used by the NFI, then the NFI internally generates 6 output variables:

1. limit
2. risk score
3. case importance
4. case threshold
5. case grounds
6. decline

[0144] Hereby, the limit directly represents the transaction-individual limit for the current authorization request. This transaction-individual limit is reduced by the risk score as malus ("floating transaction limit").

[0145] The NFI now decides by a simple comparison whether a referral has to be generated or not. A referral is always then generated when the amount requested for authorization is above the transaction-individual limit. By the variables "referral interlock" and "referral_until", the NFI decision can be modified.

[0146] The other three variables represent the NFI decision relative to the case generation. The case importance represents to which extent the current authorization request is supposed to be generated as a case. If this value is above the case threshold, than a case will be generated for the authorization. In addition, as the grounds of the decision to generate a case from this authorization message, a text "case class" will be generated describing the kind of suspicion with words. This description is used by the staff members of the Investigation Workflow for being able to carry out a targeted investigation.

[0147] These NFI output variables are transferred directly with the overall information as to the authorization, to the authorization request. The existing authorization software then processes this information further.

[0148] After the computing by the NFI, the NFI transfers the updated time series to the system. The system stores it in the Cardholder File for transferring it again to the NFI upon the next authorization request of this card number.

[0149] The actual decision rules of the NFI are recorded in a file on the authorization computer. The development tool on the PC generates this file.

[0150] In the following, the decision logic will be explained in more detail. Thereby, the following abbreviations will be used:

Table 1

AvailBal	Amount still available on the card,

	in Euro
Amount	Amount requested for authorization (in Euro)
BranchCode	Single branch codes
Branch class	Class of the branch to which the VP belongs
CountryCode	Country code from authorization message
CurrencyCode	Currency code from authorization message
GAC	Action code from list definition
ICA_BIN	Origin of transaction
Availment	Still to be defined!
Card age	Age of the card in days, measured in time that has elapsed since "valid as of new"
Card limit	Limit of card in Euro
KI_Range	Association of the card number to ranges that are defined as list
Last answer	How long ago is the last answered Referral/Callme?
Last GAA	Time elapsed since the last GAA withdrawal
Last Referral	How long ago is the last Referral/Callme?
Client	Client identification
Merchant_ID	Merchant ID from list definition
Panic factor	Still to be defined!
POS_Entry	Input kind of authorization request
Terminal_ID	Terminal ID from list definition
Z01	Input variable of counter XXXX
Z02	Input variable of counter XXXX
Z03	Input variable of counter XXXX
Z04	Input variable of counter XXXX
Z05	Input variable of counter XXXX
Z06	Input variable of counter XXXX
Z07	Input variable of counter XXXX
Z08	Input variable of counter XXXX
Z09	Input variable of counter XXXX
Z10	Input variable of counter XXXX
Z11	Input variable of counter XXXX
Z12	Input variable of counter XXXX
Time series length	Number of authorization requests currently stored in time series
Decline	Generation of a "hard" decline
Case class	Declaration which Fraud Supervisory and Fraud Investigation "transfers" so as to depict why exactly this case has been generated
Case threshold	This is the possibility to define in FuzzyTECH "variably" a threshold for the case generation
Case importance	Degree to which the current authorization request is being regarded as "caseworthy"

GansLimit	Transaction limit (determined as per user rules (in Euro))
RiskScore	Risk score which is taken as a basis for determining the "malus" in the floating transaction limit
Rule Limit	Transaction limit (determined as per user rules)
Calculate MBF	Calculate Membership Function (fuzzification method)
CoM	Center of Maximum (defuzzification method)
MoM	Means of Maximum (defuzzification method)
Default	Setting of a process variable (visualization interface)
BSUM	Bounded Sum – Operator for calculating the result aggregation
MIN	Minimum Operator (AND-aggregation)
MAX	Maximum Operator (OR-aggregation)
GAMMA	Compensatory Operator for aggregation
PROD	FuzzyOperator for composition
LV	Linguistic variable
MBF	Membership Function
RB	Rule Block

[0151] The system structure describes the data flow in the fuzzy system. Input interfaces fuzzify the input variables. Hereby, the analog values are converted into association levels. The fuzzy interference follows to the fuzzification: With "IF-THEN" instructions fixed in rule blocks, linguistically described output variables are fixed by the input variables. These are transformed in the output interfaces into analog variables by a defuzzification.

[0152] Figure 5 shows the structure for this fuzzy system having input interfaces, rule blocks and output interfaces. The connection lines hereby symbolize the data flow.

[0153] Linguistic variables serve in a fuzzy system for describing the values of continuous variables by linguistic terms. The possible values of a linguistic variable are not digits, but linguistic notions, also called terms.

[0154] For all input, output and intermediate variables of the fuzzy system, linguistic variables are defined. The association function of the terms are uniquely fixed by support points, the so-called definition points.

[0155] The following table lists all linguistic variables together with the term names.

Table 2: Linguistic variables

AvailBal	Low, medium, high
Amount	Low, medium, greater_1000, high
BranchCode	Airport general, store, furs, carpets, sound records, night bars, arms dealer, jeweler, photo, leather, all banking, Hotel general, all 5-type MCCs, massage, automobile general, fun leisure
Branch class	Hotel, airlines, automobile, Buizserv, car_rentals, cashing, clothing, contrctd_services, mail_order, misc_store, non 5311, pers_services, retail, services, transportation, utilities, -cashing
CountryCode	Egypt, Brazil, Ecuador, Hongkong, Indonesia, Israel, Colombia, Malaysia, Marocco, Mexico, Singapur, Thailand, Turkey, Venezuela, Canada
CurrencyCode	F_franc, olden, forinth, olden, i_lira, peseta, pound
GAC	bad_cvc
ICA_BIN	Visa_quer, mexico_special, -mexico_special
Availment	Low, medium, high
Card age	Very_new, new, old
Card limit	Low, medium, high
KI_Range	No_range, fraud_nz, all_others
Last answer	Just_now, v_long_ago
Last GAA	Just_now, medium, long_ago
Last Referral	Just_now, v_long_ago
Client	No_client, gzs, airplus
Merchant_ID	Wempe
Panic factor	Low, medium, high
POS_Entry	Unknown, unknown_o_manually, manually, read, electr_commerce, read_checked
Terminal_ID	Crimin_figaro
Z01	more_than_four
Z02	more_than_four
Z03	more_than_four
Z04	more_than_four
Z05	more_than_four
Z06	more_than_four
Z07	more_than_four
Z08	more_than_four
Z09	more_than_four
Z10	more_than_four
Z11	more_than_four
Z12	more_than_four

Time series length	High
Decline	No_decline, decline
Case class	Counterfeit, hongkong, cvc_queue, hungary, watchlist, jewelers
Case importance	Unsuspicious, medium, suspicious
Limit	_0, _100, _250, _500, _1000, _2500, _7500
RiskScore	Unsuspicious, medium, suspicious
profile	Unsuspicious, medium, risky
Rule limit	_0, _100, _250, _500, _1000, _2500, _7500

[0156] The qualities of the basis variables are listed in the following table.

Table 3: Basis variables

Variable name	min	max	default	Unit
AvailBal	0	20000	0	Euro
Amount	0	20000	0	Euro
BranchCode	0	9999	0	MCC
Branch class	0	32	0	codevalue_list
CountryCode	0	999	0	CC_key
CurrencyCode	0	999	0	CC_key
GAC	0	32	0	codevalue_list
ICA_BIN	0	32	0	codevalue_list
Availment	0	100	0	percent
Card age	0	100	0	days
Card limit	0	20000	0	Euro
KI_Range	0	32	0	codevalue_list
Last answer	0	45	45	days
Last GAA	0	45	0	days
Last Referral	0	45	45	days
Client	0	32	0	codevalue_list
Merchant_ID	0	32	0	codevalue_list
Panic factor	0	100	0	percent
POS_Entry	0	32	0	POS_Entry_Mode
Terminal_ID	0	32	0	codevalue_list
Z01	0	32	0	number
Z02	0	32	0	number
Z03	0	32	0	number
Z04	0	32	0	number
Z05	0	32	0	number
Z06	0	32	0	number

Z07	0	32	0	number
Z08	0	32	0	number
Z09	0	32	0	number
Z10	0	32	0	number
Z11	0	32	0	number
Z12	0	32	0	number
Time series length	0	32	0	AuthoriRequests
Decline	0	1	0	-
Case class	0	32	0	codevalue_list
Case threshold	0	1000	750	threshold
Case importance	0	1000	0	per mil
Limit	0	30000	0	Euro
RiskScore	0	1000	0	per mil

[0157] The default value is adopted by the output variable, when no rule fires for this variable. Various methods can be used for the defuzzification, which either furnish the "most plausible result" or the "best" compromise.

[0158] To the compromise-forming methods belong:

CoM (Center of Maximum)

CoA (Center of Area)

CoA BSUM, a variant for efficient VLSI implementations

[0159] The "most plausible result" is furnished by:

MoM (Mean of Maximum)

MoM BSUM, a variant for efficient VLSI implementations

[0160] The following table lists all variables linked with one interface, as well as the corresponding fuzzification or defuzzification method.

Table 4: Interfaces

Variable name	Type	Fuzzification/defuzzification
AvailBal	Input	calculate MBF
Amount	Input	calculate MBF

BranchCode	Input	calculate MBF
Branch class	Input	calculate MBF
CountryCode	Input	calculate MBF
CurrencyCode	Input	calculate MBF
GAC	Input	calculate MBF
ICA_BIN	Input	calculate MBF
Availment	Input	calculate MBF
Card age	Input	calculate MBF
Card limit	Input	calculate MBF
KI_Range	Input	calculate MBF
Last answer	Input	calculate MBF
Last GAA	Input	calculate MBF
Last Referral	Input	calculate MBF
Client	Input	calculate MBF
Merchant_ID	Input	calculate MBF
Panic factor	Input	calculate MBF
POS_Entry	Input	calculate MBF
Terminal_ID	Input	calculate MBF
Z01	Input	calculate MBF
Z02	Input	calculate MBF
Z03	Input	calculate MBF
Z04	Input	calculate MBF
Z05	Input	calculate MBF
Z06	Input	calculate MBF
Z07	Input	calculate MBF
Z08	Input	calculate MBF
Z09	Input	calculate MBF
Z10	Input	calculate MBF
Z11	Input	calculate MBF
Z12	Input	calculate MBF
Time series length	Input	calculate MBF
Decline	Output	MoM
Case class	Output	MoM
Case threshold	Output	default
Case importance	Output	CoM
Limit	Output	MoM
RiskScore	Output	CoM

[0161] Rule blocks

[0162] The controller behavior in the various process situations is fixed by the rule blocks. Each single rule block contains rules for a fixed set of input and output variables.

[0163] The "IF" part of the rules thereby describes the situation in which the rule is supposed to be valid; the "THEN" part describes the reaction thereto. By the "Degree of Support" (DoS), the single rules can be imparted a varying weighting.

[0164] For evaluating the rules, the "IF" part is first calculated. Hereby, various methods can be used, which are fixed by the operator type of the rule block. The operator can be of the MIN-MAX, MIN-AVG or GAMMA type. The operator behavior is in addition influenced by a parametrization.

[0165] For example:

MIN-MAX having the parameter value 0	=	Minimum-Operator (MIN).
MIN-MAX having the parameter value 1	=	Maximum-Operator (MAX).
GAMMA, having the parameter value 0	=	Product-Operator (PROD).

[0166] The Minimum-Operator is the generalization of the Boolean "AND", and the Maximum-Operator is the generalization of the Boolean "OR".

[0167] The results of the single rules are summarized in the subsequent fuzzy composition to overall conclusions. The BSUM method hereby considers all rules firing for one condition, whereas the MAX method takes only dominant rules into account.

What is claimed is:

1. A method which is implemented on a computer and which is provided for identifying and determining fraudulent transaction data in a computer-controlled transaction processing system comprising a prediction model for receiving current transaction data, for processing the current transaction data, and for outputting at least one output value that depicts a probability of a fraudulent transaction, wherein, on the basis of stored data, for

- a time series analysis of earlier transactions with respect to the same means of payment or user, and
- expert rules concerning parameters which occur in a statistically significant cumulative manner during fraudulent transactions, especially with respect to the origin of the means of payment/user, to the branch and to the beneficiary of the transaction, as well as to the magnitude or value of the transaction, the evaluation is carried out by means of the prediction model with respect to the risk of the current transaction being fraudulent, and a corresponding output value is generated,

wherein the prediction model combines a limit, which is essentially based on the expert rules and which is specific for the type of transaction, with a value, which is essentially based on the time series analysis and which is specific for the current transaction, in order to generate the output value,

the combination being carried out in a floating manner so that output values can be generated which vary according to the extent of the suspicion of misuse and which can be used to initiate different reactions to the current transaction request.

2. The method according to claim 1, wherein the time series analysis is implemented in the form of fuzzy logic rules.

3. The method according to claim 1 or 2, wherein the expert rules are implemented in the form of fuzzy logic rules.

ABSTRACT OF THE DISCLOSURE

A method and system for identifying and determining fraudulent transaction data in a computer controlled transaction processing system using a prediction model. The prediction model is used to carry out the evaluation with regard to the risk that the current transaction is fraudulent, and a corresponding output value is generated. This evaluation is carried out using stored data of a time series analysis of earlier transactions and to expert rules concerning parameters which occur in a statistically significant cumulative manner during fraudulent transactions. The prediction model combines a limit with a value in order to generate the output value. The combination is carried out in a floating manner.

TRANSLATION OF INTERNATIONAL APPLICATION

EXPERT SYSTEM

The invention relates to the detection of the fraudulent use of customer accounts and account numbers, including, for example, transactions with credit cards. The invention in particular relates to an automated fraud detection system and a method using a prediction model for the pattern recognition and classification so as to pick out transactions having a high likelihood of fraud. In the following discussion, the term "credit card" will be used for descriptiveness purposes; the here discussed methods and fundamentals, however, apply as well to other kinds of electronic payment systems, such as, for example, customer credit cards, automated machine-readable cash cards and telephone cards.

The establishments issuing credit cards have at all times tried to restrict their losses caused by fraud in that the fraudulent use of the card is indicated before the card holder has notified a lost or stolen card.

An effective model for the fraud detection was supposed to result in high catch rates at a low impediment of legal transactions in the real time operation. It was supposed to be able to adapt to changing fraud methods and patterns, and was supposed to have an integrated learning capacity supporting this capacity of adaptation.

The prior published specification WO-A-8 906 398 describes an element for the analysis of a transaction by means of data processing: in that only that data is extracted, which is useful for the analysis of the transaction; in that signals are cancelled corresponding to a transaction which is presumed to match with a set of predetermined rules; in that it is filtered so as to eliminate non-significant modifications of the transaction to be analyzed; and in that signals are classified into one or several classes according to a predetermined criterion. This element is suited for the application of issuing payment authorizations to credit card users.

A further specification, EP-A-0 418 144, describes a method for restricting the risks associated with a computer-assisted transaction, in that the transaction request is compared to predetermined statistical data, which seems to be representative of a risk score of a non-

conform use. The statistical data describes the mean number or the quantity of transactions performed during the sequence of successive periods of time, and is derived in that the time is divided into successive, non-equal periods, the duration of which are selected in a manner that the likelihood of a performed transaction or the mean amount for each single period of time are substantially equal.

From EP-0 669 032, a fraud detection method implemented on a computer, and a corresponding hardware are known, which includes means for prediction models. Current transaction data is received and processed, which then results in a plurality of output values containing a hit value representing the likelihood for a fraudulent transaction.

This method known in the prior art requires several steps, which have to be carried out prior to the processing steps for the current data, namely:

- generating a user profile for each individual of a plurality of users out of an enormous number of variables relative to previous transactions, and of personal user data containing for each user values out of a plurality of user variables, each user profile defining a pattern for the transaction history of a user;

- deriving variables concerning proven previous fraud in that data of previous transactions are preprocessed, these values containing a plurality of previous transactions for a plurality of transaction variables;

- training of means for prediction models with said user profiles and said variables concerning previous fraud, so as to obtain a prediction model; and

- storing said obtained prediction model in the computer.

Then, the processing of the current data is carried out in that

- the current transaction data for a current transaction of a user is received;

- the user data concerning the user, is received;

- the user profile associated with the user, is received;

- the obtained current transaction data, user data and the user profile are preprocessed so as to derive variables relative to a current fraud for the current transaction;

- the likelihood of fraud in the current transaction is determined in that the prediction model is applied to the current fraud-related variables; and

- an output signal is emitted from the means for the prediction model, which signal indicates the likelihood of fraud for the current transaction.

This system supports on a neuronal network for training the means for the prediction model. Said training is supposed to mainly change the means for the prediction model so as to keep the prevention of legal transactions low, and to improve the performance of the system for the detection of fraud.

Hereby, the system supports on a set of fixed (yet variable) values representing various aspects of the transaction. These values are differently weighted in processing, and one important function of the training based on the neuronal network, is the variation of said weighting, basically resulting in a "learning" capacity for this system. Such known neuronal networks represent a linking of "neurons" in the meaning of simple mathematical transfer functions. For generating a "learning capacity" here, a corresponding algorithm is used – e.g. according to EP 0 669 032, for adapting the "weights" with the data rating in the neuronal network.

In spite of all that, the system for combining the different parameters and data, employs usual logic algorithms and functional relationships for obtaining the hit value. For each current

transaction, it carries out a calculation based on conventional logic, views the results (later), and varies, if necessary, the algorithm.

It is desirable to create an automated system which uses the available information, e.g. on the card holder, merchants and shops for monitoring transactions and picking out these which are probably fraudulent, and which is able of thereby discovering a relatively higher portion of cases of frauds at a relatively lower prevention of legal transactions. Such a system should preferably also be capable of dealing in a fast real time operation with a large number of variables independent of each other, and should feature the capacity of redeveloping the basic system model as new patterns for upcoming fraud behavior.

The invention accordingly relates to a computer-implemented method for identifying and determining fraudulent transaction data according to the features of claim 1.

To some extent, the invention uses features known from EP 0 669 032. Reference is therefore made to the complete scope to EP 0 669 032.

As can be seen from the following description, there exist, however, major differences between the invention and this prior art, residing in the basic approach and in the corresponding basic structure, as well as in various details of the data generation and processing.

An essential difference results from the fact that the present invention does not use a user profile as a part of the prediction model. Instead, the invention works with a combination of expert rules, for one, and an analysis of preceding operations of using the payment means, for another, which is used for the transaction to be currently evaluated.

Comparable to the initially mentioned prior art, the expert rules concern a selection of typical elements of an individual transaction based on experience values, i.e. the analysis of past cases of misuse, which elements are indicative for an increased risk of misuse. According to

the invention, the origin of the payment means is in particular relevant (e.g. the card), the branch and the person beneficiary of the payment to be authorized, and the payment amount.

The analysis of preceding events of use of the same payment means preferably comprises the latest events, for example, the last five to twenty transactions (this could, however, also go further back).

In contrast to the prior art as per EP 0 669 032, the invention preferably does not use a conventional neuronal network in combination with a learning algorithm.

The invention uses fuzzy logic for determining whether a certain transaction has to be considered as being fraudulent.

In the decision system preferred according to the invention, the expert rules, as well as the rules functionally corresponding to the prior art neuronal network, are memorized for the descriptive statistics as fuzzy rules, and therewith do not differ in the calculation method, but in the gaining method.

The expert knowledge is directly formulated as fuzzy rules. These define a limit for each transaction type that corresponds to the (user-specific) "risk readiness".

The information from the use history of the payment means is likewise transformed into fuzzy rules by means of a "NeuroFuzzy module". The NeuroFuzzy module uses a modification of that training algorithm, which is also used in most neuronal networks, namely the Error Backpropagation algorithm to a large extent described in the literature. Since in this way the information from past data (hence that, what is, for example, memorized in the weights of the trained neuronal network according to EP 0 669 032) is available as readable and interpretable/modifiable fuzzy rules, this information can be completed, verified and extended in any manner. With respect to the input and output data, the "neuronally" generated fuzzy rules can use the same variables as the expert rules.

The "neuronally" generated fuzzy rules are preferably based on an analysis of preceding transactions with respect to such factors as the average transaction amount, the portion of cash disbursements, the portion of foreign jobs, of travel cost use, the previous occurrence of suspicious cases, etc., and with respect to "dynamic" criteria such as, for example, the current exhaustion of the limit of the credit card concerned. The result of this analysis is also designated as "time series". This rule system thus assesses a dynamic risk for each transaction in the form of a "bonus" or a "malus".

Thus, the invention permits the merging of statistical models with expert knowledge. Instead of simply calculating for each event, as it is the case with prior art, a fraud probability, the limit defined for each transaction type, is floatingly combined with the dynamic risk ("bonus" or "malus") of the specific current transaction to a (floating) transaction limit.

This enables various differentiated treatments of "eye-catching" transactions, e.g. the immediate interlock, or instead, the remittance for an individual check, e.g. through a person in charge.

In the prior art, a transaction lying above the risk threshold normally is stopped; the prior art basically only knows the release or interlock as a result of the check. The invention instead enables gradual reactions; for example, a suspicious case can be generated (and therewith enter into the "time series" for this credit card, which will be referred to for future transactions), although the current transaction is being authorized. In case of a stronger suspicion, a re-check (referral) of the current transaction would be initiated (prior to the possible authorization thereof); with a still stronger suspicion, the transaction would be rejected (decline).

Substantial differences to the prior art also result with respect to the model formation, hence, the generation and recognition of misuse patterns (fraud patterns).

The prior art is based on a "passive data gain". In other words, exclusively already present past data is referred to for the model formation. This means that, for being able to recognize a

fraud pattern in the model at all, (a) a sufficiently long time must have elapsed, so that the fraud messages have already come back (in most cases only after the customers have read their statement of accounts), (b) enough cases for a secure training must be given (a neuronal network functions only in this case / there exist fraud cases which are very rare but cause a high individual damage, and which are only very difficult to cover in the model, (c) an immunization of the authorization operation is only possible at all after laborious manual retraining.

The data gain according to the invention, however, is "active". If the first suspicious factors of a new fraud pattern arise, then new rules will be defined immediately initiating an investigation of exactly these cases by actively contacting the customers. Thus, many secured data will be available within a few hours in the ideal case as to whether a new fraud pattern has actually arisen, and how it differentiates from other patterns. This analysis (it makes no difference by means of which method) namely can only then be carried out when enough secured data is present.

The methods of the prior art model establishment leads to the fact that the experience of human analysts cannot sufficiently be used, and expectations as to future fraud patterns cannot gain entry. In the prior art, the neuronal network virtually constitutes a "black box" of fixed, rigid criteria, which still are only modified "automatically" with respect to their "weights", hence, as the result of algorithms in turn fixed beforehand. As far as expert rules are used at all together with neuronal networks, neuronal network and expert rules run independently side by side. Through the NeuroFuzzy approach, the predictive model trained with data, is no longer a black box, but is generated in the form of fuzzy rules. These can be directly interpreted and modified by experts.

The floating transaction limits according to the invention permit an efficient combination of "hard facts" and "soft facts". This enables the "soft" and "hard" facts to be modeled in a consistent and cooperative way. With the prior art "black box" approach, this is of no importance, since there, no knowledge-based modelling takes place. With the invention which

enables and preferably also provides that an automatic model formation and human expertise are combined in the running operation, this is very relevant.

The invention will be explained in more detail in the following by means of an exemplary embodiment comprising configurations of the inventive basic principle particularly preferred at present.

The exemplary embodiment relates to an authorization system for credit card transactions, and therewith to a basic constellation similar to that of the initially discussed state of the art. From an existing network comprising points of use for the credit cards usable in the system, come authorization requests which have to be handled and answered in real time.

The handling of the authorization requests takes place in the inventively configured authorization system schematically shown in the Figures 1 through 4.

In the exemplary embodiment, the system comprises several computers but can of course also be realized on a central computer or by means of a computer network.

In the example, the system comprises a "tandem" computer with a database A, an "SGI" server (SQL server) with a database B, and a "host system" with a database C.

On the tandem computer, a software is implemented serving for data transfer, data reprocessing (criteria derivation), time series calculations and time series updates, etc., as will become clear later. Moreover, the inventive decision logic is implemented on the tandem computer, including fuzzy expert rules and NeuroFuzzy models, and making the decision on authorization requests. The software implemented on the tandem computer in summary will be designated "NeuroFuzzy Interference Machine" (NFI) in the following.

The SGI server, if the case may be in conjunction with a corresponding number of PC clients, serves in particular for the implementation of the software for the "Investigation Workflow"

(IW) for the follow-up on cases of suspicion, and for the "Online Data Mining Module" (ODMM), as will be explained later.

The host system contains and receives the essential historic and current data as to payment means and user, required for the treatment of the authorization requests.

Figure 1 shows a principal information exchange as follows:
The authorization system obtains data (1) for a cardholder file from database [C] of the host system. With a modification of the data of the cardholder file, only the data of a card number relevant for the authorization is transferred to the authorization system. Events such as card interlocks having a high priority, are immediately transferred, others having a low priority, are transferred only much later. The data transfer (update) takes place hourly.

The SGI server receives (2), via the existing network, the authorization requests from the authorization tandem computer provided with the NFI-initiated action (same is comprised of: case importance, case class, case threshold, referral decision, risk score, limit and action code), as well as the current time series information. (The real time requests necessary for this purpose are in the range of minutes. The overall information as to an authorization request is compressed to a message by the NFI, which message is then transferred to the SGI server).

The SGI server further receives from the host system any posting information, misuse information and, if the case may be, card holder main data, which cannot be extracted from the cardholder file (3). The database of the SGI server [B] stores this data as long as required, depending on the storage expansion. The SGI server lodges the server component, be it of the Supervisory Workflow (ODMM) or also of the Investigation Workflow (IW).

Figure 2 shows the data flow with presumed or recognized misuse cases.

The Investigation Workflow (IW) (6) serves for the treatment, in particular by means of staff members (Call Center), of recognized and presumed fraud cases.

In the Call Center, it is ascertained whether the presumed cases of misuse actually are cases of misuse. A corresponding information (7) to the SGI server takes place.

Apart from this main task, the SGI server fulfils still another main task:

The SGI server database stores the data necessary for the discovery of new fraud patterns, and processes same for an analysis by the Online Data Mining Module (ODMM). For this purpose, the misuse-relevant data is buffered in database [B]. In the Fraud Supervisory Center, new fraud rules are then defined by means of this information (4), and the existing fraud rules are continuously checked for their efficiency.

The correspondingly modified fraud rules in the form of a file are then transferred from the Fraud Supervisory Center to the authorization computer (5). For doing this, the file is brought to the SGI server from the PC. On the SGI server, an automatic job is installed which recognizes when the time stamp of the file has changed, and performs an exchange of said file on the tandem in this case and also communicates to the NFI that has to read-in this file anew.

Hence, two workflows result *in toto* (Figure 4):

1. The Supervisory Workflow ODMM adapts continuously the decision strategy of the prevention system to the changing misuse patterns.

2. The Investigation Workflow IW checks the decisions of the prevention system by individually treating the reported and presumed cases of misuse.

Both Workflows are indirectly connected via the (mean) operative EDP level. If the decision strategy is modified in the Supervisory Workflow, then other referrals will be generated by the prevention system, which will be investigated in the Investigation Workflow.

A misuse not timely recognized by the prevention system, as well as an erroneous misuse presumption, is verified by the Investigation Workflow and stored in the database of the SGI

server. Hereto accesses the Online Data Mining Module (ODMM) and proposes a corresponding modification of the decision strategy to the fraud experts in the Fraud Supervisory Center.

The overall calculation, hence the flow of the fuzzy interference through the rule work, as well as the entire profile formation and initialization, is taken over by the NFI itself; an external control is not required. The interface contains further functions for the initialization and configuration of the decision logic (these functions have to be invoked once upon loading of the prevention module), which, however, have not to be invoked per authorization request.

The SQL database of the authorization computer (Cardholder File) is supplemented by a field "time series". This field stores the last authorization requests to this card number (profile of use) in a compressed form. When an authorization request enters the system, the complete data set of the card is loaded from the database. Here, the binary object "time series" has in addition to be loaded from the database and transferred to the NFI. The binary object profile of card use is then generated in an extremely compressed form, so that is can be efficiently stored in the SQL database for the real time access. Additional computing time by the read-out and re-storage of the card profile upon each authorization request, will not cause a noticeable computing effort, since the data set of a card is in any case read out upon each authorization request. After the decision, the NFI updates the time series by the authorization just received. Exactly as the limits updated by the authorization, the updated time series has to be written back into the database, as well.

Furthermore, the Cardholder File is supplemented by two date fields, in each case one for "no referral until" (this field is set upon a positively answered referral for ensuring that, immediately after a positive ID, the card holder directly receives again a referral on the occasion of the next transaction), and one for "short referral until" (upon an acute suspicion, this date is set so as to forcibly generate a referral with each authorization request up to this date). These fields are set or reset through the authorization system. The data is delivered to the NFI by the authorization system, the NFI evaluates the data and decides whether a referral or decline or, if the case may be, a case shall be generated. Since the NFI, if the case may be,

also contains client-dependent rules, the NFI has to recognize the client from the card number. (A client is, for example, the client of the processing company, for whom the fraud processing is carried out).

The development component is part of the Supervisory Workflow and a graphical development and analysis software, which is installed on Windows/NT workstations (clients). Hereby, existing computers can be concerned which are also used for other tasks, or a separate computer can be provided.

Proceeding from the development software, the developer can modify the fuzzy decision system of the tandem. Hereby, the ongoing authorization process is in any case neither stopped, nor disturbed nor decelerated.

If new fraud patterns become known, then the development component allows to take same into consideration by modification of known and definition of new rules. Thereby, these new rules and modified rules are transferred to the NFI, where the new rules have an instantaneous effect on the authorization behavior.

All authorization requests are handed over by the tandem to the SGI server via TCP/IP. The SGI server establishes a new record for each authorization request, and fills same with all necessary information.

If the case importance of an authorization request is above the case threshold, then the SGI server establishes a case in addition. A case is comprised of an entry in the case table and the associated sub-tables.

In summary:

Each message incoming from the tandem describes an authorization request.

A record is established for each authorization request.

The case generation is independent of the referrals, i.e., a case may be generated without a referral having been generated, and a referral may be generated without a case being generated.

This interface is installed on part of the SGI servers. Likewise is the generation of the corresponding entries in the SGI server tables.

The Investigation Workflow serves for following up the possible fraud cases and referrals. Hereby, the case importance ascertained by the NFI is taken as a basis for the case grading. Whether a referral has been generated for this authorization request or not, is not important for the generation of a case. The case generation works with its own decision logic, which can also contain rules deviating from the fraud rules. Prevention strategies can hereby be tested so to speak, as a "dry run". Therewith, also such cases can be followed up in the Investigation Workflow, in which the suspicion did not suffice for a referral generation.

Compressed storage of the authorization history ("time series")

The NFI works with neuronal models which are based on the analysis of previous transactions.

The problem of such an analysis is that during the treatment of an authorization request, a polling and analysis of past transactions is not possible in real time. Therefore, the NFI has to store a brief history temporarily in a ring buffer. (A ring buffer is a storage having a fixed number of places switched in series. Each newly stored object is pushed into the ring buffer "at the front", thus advancing all objects already present in the ring buffer in each case by one position. The object in the last place thereby completely falls out of the ring buffer.) It is of particular importance here that the time series requires as little storage place as possible (each byte per card results in a net storage place requirement of about 7 megabyte in the database of the authorization computer), and that it is allowed to be read and written as fast and efficiently as possible.

The time series formation is for this reason based on an algorithm, which generates and updates said ring buffer in such a manner that it is efficient to store and compute. For the storage, a compressed memorization in the converted integer format is used.

The time series information thereby represents, for example, a condensed history of the last 15 authorization requests, which enables a calculation of dynamic criteria (exhaustion, panic, gas station use, etc.) The time series information in addition permits the assessment of aggregated variables such as: average shopping amount, cashing portion, foreign country portion, travel cost use portion, when has a referral been issued for the last time, and when has a referral been answered for the last time.

Since the time series information has to be stored (in the ring buffer for each authorization request) 15 times, a compression of the information is particularly important.

Since the profile is stored in the database as binary object (string format), the individual partial information of each transaction can be coded in the ring buffer as integers of an arbitrary bit length. However, a reasonable division of individual bit lengths to the bytes of the string format has been chosen for keeping the calculation and update of the profiles from becoming computationally not too laborious. Hereby, the shortest possible storage form "exact bit" is not always chosen, rather there results a compromise of storage place requirement minimization and computational performance maximization.

As to the stored fields in detail:

- Date

The storage of the date in the minute format enables the simple calculation of time differences in integer arithmetic of a 16-bit digit (with a 16-bit-minute resolution, a maximum of 45 days can be represented, which is sufficient for the calculation of time differences in the profile).

The 16-bit values resulting with the subtraction of such minute values for the time differences, are directly used as input variables of the NFI without any expansive computationally scaling modifications.

With the maximum storage length of the minute date after a deadline of 24 bits, however, a reset of the profile information has to ensue every 31 years.

If this entry "date" is equal to "0", then this means that said entry is not yet used in the ring buffer.

- Amount

Has to be divided by 10 so as to result in the Euro amount. Hereby results an optimized utilization of the 20-bit digit range.
Deviations in the amount of below Euro 0.10 are unimportant for the misuse prevention, and the maximally representable amount of over Euro 100,000.00 is also sufficient. Requested values of over Euro 100,000.00 are cut down in the ring buffer to Euro 100,000.00.

- MCC

Contains the branch code of the contractual partner who has requested the authorization.

ICA

Describes all issues by means of their ICA numbers.

Country code

For the time series inspections, the country code is sufficient for the origin determination. Same is maximally three-digit, therefore 10 bits are sufficient for the representation (according to MC Quick Reference Booklet, October 97).

- POS

Receives the 5 possible POS Entry modes. 3 bits, it is true, would suffice so as to depict said 5 possible POS Entry Modes, the representation in 4 bits, however, offers arithmetic advantages.

- Status

Status describes, for example, whether the expiration date was wrong, or whether a CVC problem has arisen, etc.. (On the magnetic card, the card number is extended by a three-digit code (CVC-1). This three-digit code is not calculable. Therewith, a quite good identification of a genuine card is possible by means of this examination.) It is hereby guaranteed that non-authorized requests can be taken into consideration in the profile.

Fraud Supervisory Workflow

The Fraud Supervisory Workflow includes all tools which are used for controlling the decision logic and for waiting. In detail, these are the modules:

- Online Data Mining Module

For the systematic recognition of new misuse patterns, as well as for the continuous check of the hit security of currently defined decision rules.

- Decision logic

In this module, the decision components are developed, monitored and controlled.

- Analysis NFI

The analysis NFI serves for testing new decision logics on past scenarios.

Online Data Mining Module (ODMM)

The Online Data Mining Module is comprised of a server component on the SQL server, as well as of a client component on a PC. The client component cooperates with the server via Pass-Through Queries and linked tables.

The ODMM works with tables in which the authorization requests and cases necessary for the analysis are recorded.

The ODMM Client contains the following information as to each transaction:

- card number (together with the date and time of the transaction, this information serves for the unique allocation of each transaction (key). Since several events (e.g. several authorization requests, misuse messages, answered referrals, etc.) may belong to a transaction, which can take place at different times, the earliest date will always be used here. This corresponds to the logic that the events belonging to this transaction all refer to the first payment request, which has become known in the system.

- Date and time of the transaction

- Amount in Euro

- Type of transaction (authorized or non-authorized transaction; with non-authorized transactions, for example, no authorization request exists, a posting and a misuse message, however, can be present)

- Misuse (has misuse occurred?)

- Referral (has a referral been generated, if yes, how was it answered)

- Information from the authorization request or the posting (branch code, Country Code origin, POS Entry)

- Random number (selection of a sampling quantity)

The tables supplying this information, are polled by the ODMM Clients via Pass Through Queries.

The server allocates posterior incoming misuse messages to transactions already entered in the TRX table. The results are likewise updated for the statistic component.

- Systematic search

The systematic search runs on the server as Pass-Through Query and generates a table comprising rules which are currently not activated, and which would be reasonable to be included. A misuse amount is allocated to each rule, which could have been prevented during the examination period if this rule had been active. For verifying this statement, each rule also contains the ratio of erroneously versus legitimately refused authorization requests (F/P rate), the number of illegitimate referrals, which enable the judgment as to adoption or refusal of the rule. It is possible to filter the rules in advance by indicating a determined misuse amount and F/P rate. With smaller amounts or higher F/P rates, the found rules are blinded out. The weighting between the misuse amount and the F/P rate can be set during the classification. Therewith, it can be fixed anew with each systematic search, of which importance each of the two variables is supposed to be for the examination.

- Rule optimization

The negatively answered referrals which could not confirm a misuse, serve for the recommendation to deactivate rules as a basis. If a referral is answered negative, then the

associated data set will no longer flow into the analysis as a misuse, but as a good transaction. If it turned out then that the rule has not prevented enough misuse and has prevented many good transactions, then it will be proposed to be deactivated. In this analysis, too, the weighting between the misuse amount and the F/P rate can be set. Therewith, it can be fixed anew with each systematic search, of which importance each of the two variables is supposed to be for the examination.

Decision logic

The access to the decision logic ensues over the Fraud Supervisory Workflow:

The block "Fraud Supervisory Workflow" represents the PC networks in the staff SI. These administer decision logics of an arbitrary number, be it for the filing or as intermediate development stages. (The actual data for the decision logics are centrally stored on the SGI server, so that all fraud analysts have access to same. The access to these decision logics takes place by the PCs with the help of the "Fraud Supervisory Workflow" software.) Each of the decision logics is comprised of the three components, lists, time series and rules. By pressing the respective keys, the corresponding editors for the components will open.

In the productive operation the decision logic "Operation" always runs . By pressing the key [transfer], the decision logic "Operation" currently developed in the PC, is transferred to the tandems, and is activated.

The two decision logics for the analysis of scenarios run on the SGI server. By pressing the key [transfer], the decision logic "Test" currently developed in the PC, is transferred to the SGI servers, and is activated.

Proceeding during the development

The basic proceeding during the development of decision logics is the following. The decision logic "Operation" runs on the authorization computer. By pressing the key [transfer], the

decision logic "Test" will be overwritten with the decision logic "Operation". (Hereby, not a physical overwriting from the tandem to the SGI server is concerned. The SGI servers also dispose of a copy of the decision logic, whereby the overwriting is directly carried out on the SGI servers.)

The decision logic "Test" can hereby be modified on the PC, and with the assistance of the analysis NFI, the test of modifications takes place by a direct comparison of the "Test" system and the "Operation" system.

If the modifications carried out on the decision logic "Test" are successful, then the decision logic "Test" will be overwritten with the decision logic "Operation" by pressing the key [transfer]. After the new decision logic has become operational, the proceeding starts anew.

Each new transaction is provided with a judgment of case worthiness by the NFI machine. An auxiliary module marks a transaction as a case, when said transaction fulfils a case criterion (MCC, ICA, CNT, POS, amount class, case worthiness).

Optionally, it can be determined how far the history of the transaction and the posting of an event reaches back. A period of 4 – 6 weeks is considered to be reasonable.

If a transaction belongs to a category of all possible cases, then a new record will be established in the Investigation Workflow-inherent table. This record contains the following single data:

- card number
- transaction data (date/hour, MCC, CNT, ICA, POS, amount)
- case status (is the case new or has it been closed)
- case importance (the case importance FW represents the NFI score)
- case class (the case class indicates why a transaction has become a follow-up case or to which category the transaction belongs. The identification consequently includes indications as to MCC, ICA, CNT, POS, amount class, FW.)

- user name
- date of resubmission
- close status (the close status of a case supplies details on the result of the treatment after closing the case, and may contain the following information: "no fraud", or "no fraud estimated", "fraud confirmation impossible" or "fraud estimated".)

The card number is the link (pointer) to the past transactions with the same card number on the DBMS of the SGI server. Together with the card number main data, all data are complete for the Fraud Investigation Workflow.

NFI input variables

The NFI is integrated into the authorization process over a token protocol. From here, the NFI takes out all input variables, as well as the time series as binary data object (string).

As a special form of authorizations, the NFI has to interpret the messages on a referral interlock or a referral_until.

Referral_until: the parameter referral_until (short referral) is used with a misuse suspicion for preventing authorizations. It is manually activated by an authorization.

The NFI memorizes the referral_until date in the card profile, and checks during the authorization whether the transaction date is smaller than the referral_until date. If this is the case, a referral will always be generated by the NFI.

The referral_until parameter is transferred for analysis and reconstruction to the SGI computer via the TCP/IP interface as a component of the transaction data set.

Referral interlock: the referral interlock is used for preventing the further initiation of referrals after a positive identification or after viewing the past transactions. The referral interlock can adopt the conditions "valid" or "not valid". If it is "valid", then a previously set parameter is

activated indicating a fixed offset from the current transaction date (e.g., transaction date + 3 days). The referral interlock is always given in the form of a date, until which it shall last. It namely can only be determined at the current moment whether the interlock therewith is valid or not.

The referral interlock can be activated, for one, proceeding from the Investigation Workflow. For another, the referral interlock can also be indirectly initiated by the authorization service, when a positive identity check has taken place after a referral. After a positive identity check, the authorization service initiates a transaction, which is processed in the NFI. The NFI writes the current referral interlock into the Cardholder File on the authorization computer.

The case has to be avoided of a referral interlock, as well as the referral_until date both being valid. For this reason, when one value is set (e.g. referral_until), the respective other value is erased (e.g. referral interlock).

Internal output variables

If all input variables are present, which are used by the NFI, then the NFI internally generates 6 output variables:

1. limit
2. risk score
3. case importance
4. case threshold
5. case grounds
6. decline

Hereby, the limit directly represents the transaction-individual limit for the current authorization request. This transaction-individual limit is reduced by the risk score as malus ("floating transaction limit").

The NFI now decides by a simple comparison whether a referral has to be generated or not. A referral is always then generated when the amount requested for authorization is above the transaction-individual limit. By the variables "referral interlock" and "referral_until" , the NFI decision can be modified.

The other three variables represent the NFI decision relative to the case generation. The case importance represents to which extent the current authorization request is supposed to be generated as a case. If this value is above the case threshold, than a case will be generated for the authorization. In addition, as the grounds of the decision to generate a case from this authorization message, a text "case class" will be generated describing the kind of suspicion with words. This description is used by the staff members of the Investigation Workflow for being able to carry out a targeted investigation.

These NFI output variables are transferred directly with the overall information as to the authorization, to the authorization request. The existing authorization software then processes this information further.

After the computing by the NFI, the NFI transfers the updated time series to the system. The system stores same in the Cardholder File for transferring it again to the NFI upon the next authorization request of this card number.

The actual decision rules of the NFI are recorded in a file on the authorization computer. This file is generated by the development tool on the PC.

In the following, the decision logic will be explained in more detail. Thereby, the following abbreviations will be used:

Table 1

AvailBal	Amount still available on the card, in Euro
Amount	Amount requested for authorization

	(in Euro)
BranchCode	Single branch codes
Branch class	Class of the branch to which the VP belongs
CountryCode	Country code from authorization message
CurrencyCode	Currency code from authorization message
GAC	Action code from list definition
ICA_BIN	Origin of transaction
Availment	Still to be defined!
Card age	Age of the card in days, measured in time that has elapsed since "valid as of new"
Card limit	Limit of card in Euro
KI_Range	Association of the card number to ranges that are defined as list
Last answer	How long ago is the last answered Referral/Callme?
Last GAA	Time elapsed since the last GAA withdrawal
Last Referral	How long ago is the last Referral/Callme?
Client	Client identification
Merchant_ID	Merchant ID from list definition
Panic factor	Still to be defined!
POS_Entry	Input kind of authorization request
Terminal_ID	Terminal ID from list definition
Z01	Input variable of counter XXXX
Z02	Input variable of counter XXXX
Z03	Input variable of counter XXXX
Z04	Input variable of counter XXXX
Z05	Input variable of counter XXXX
Z06	Input variable of counter XXXX
Z07	Input variable of counter XXXX
Z08	Input variable of counter XXXX
Z09	Input variable of counter XXXX
Z10	Input variable of counter XXXX
Z11	Input variable of counter XXXX
Z12	Input variable of counter XXXX
Time series length	Number of authorization requests currently stored in time series
Decline	Generation of a "hard" decline
Case class	Declaration which Fraud Supervisory and Fraud Investigation "transfers" so as to depict why exactly this case has been generated
Case threshold	This is the possibility to define in FuzzyTECH "variably" a threshold for the case generation
Case importance	Degree to which the current authorization request is being regarded as "caseworthy"
GansLimit	Transaction limit (determined as per user rules (in Euro))
RiskScore	Risk score which is taken as a basis for determining the

	"malus" in the floating transaction limit
Rule Limit	Transaction limit (determined as per user rules)
Calculate MBF	Calculate Membership Function (fuzzification method)
CoM	Center of Maximum (defuzzification method)
MoM	Means of Maximum (defuzzification method)
Default	Setting of a process variable (visualization interface)
BSUM	Bounded Sum – Operator for calculating the result aggregation
MIN	Minimum Operator (AND-aggregation)
MAX	Maximum Operator (OR-aggregation)
GAMMA	Compensatory Operator for aggregation
PROD	FuzzyOperator for composition
LV	Linguistic variable
MBF	Membership Function
RB	Rule Block

The system structure describes the data flow in the fuzzy system. Input interfaces fuzzify the input variables. Hereby, the analog values are converted into association levels. The fuzzy interference follows to the fuzzification: With "IF-THEN" instructions fixed in rule blocks, linguistically described output variables are fixed by the input variables. These are transformed in the output interfaces into analog variables by a defuzzification.

Figure 5 shows the structure for this fuzzy system having input interfaces, rule blocks and output interfaces. The connection lines hereby symbolize the data flow.

Linguistic variables serve in a fuzzy system for describing the values of continuous variables by linguistic terms. The possible values of a linguistic variable are not digits, but linguistic notions, also called terms.

For all input, output and intermediate variables of the fuzzy system, linguistic variables are defined. The association function of the terms are uniquely fixed by support points, the so-called definition points.

The following table lists all linguistic variables together with the term names.

Table 2: Linguistic variables

AvailBal	Low, medium, high
Amount	Low, medium, greater_1000, high
BranchCode	Airport general, store, furs, carpets, sound records, night bars, arms dealer, jeweler, photo, leather, all banking, Hotel general, all 5-type MCCs, massage, automobile general, fun leisure
Branch class	Hotel, airlines, automobile, Buizserv, car_rentals, cashing, clothing, contrctd_services, mail_order, misc_store, non 5311, pers_services, retail, services, transportation, utilities, -cashing
CountryCode	Egypt, Brazil, Ecuador, Hongkong, Indonesia, Israel, Colombia, Malaysia, Marocco, Mexico, Singapur, Thailand, Turkey, Venezuela, Canada
CurrencyCode	F_franc, olden, forinth, olden, i_lira, peseta, pound
GAC	bad_cvc
ICA_BIN	Visa_quer, mexico_special, -mexico_special
Availment	Low, medium, high
Card age	Very_new, new, old
Card limit	Low, medium, high
KI_Range	No_range, fraud_nz, all_others
Last answer	Just_now, v_long_ago
Last GAA	Just_now, medium, long_ago
Last Referral	Just_now, v_long_ago
Client	No_client, gzs, airplus
Merchant_ID	Wempe
Panic factor	Low, medium, high
POS_Entry	Unknown, unknown_o_manually, manually, read, electr_commerce, read_checked
Terminal_ID	Crimin_figaro
Z01	more_than_four
Z02	more_than_four
Z03	more_than_four
Z04	more_than_four
Z05	more_than_four
Z06	more_than_four
Z07	more_than_four
Z08	more_than_four
Z09	more_than_four
Z10	more_than_four
Z11	more_than_four
Z12	more_than_four
Time series length	High

Decline	No_decline, decline
Case class	Counterfeit, hongkong, cvc_queue, hungary, watchlist, jewelers
Case importance	Unsuspicious, medium, suspicious
Limit	_0, _100, _250, _500, _1000, _2500, _7500
RiskScore	Unsuspicious, medium, suspicious
profile	Unsuspicious, medium, risky
Rule limit	_0, _100, _250, _500, _1000, _2500, _7500

The qualities of the basis variables are listed in the following table.

Table 3: Basis variables

Variable name	min	max	default	Unit
AvailBal	0	20000	0	Euro
Amount	0	20000	0	Euro
BranchCode	0	9999	0	MCC
Branch class	0	32	0	codevalue_list
CountryCode	0	999	0	CC_key
CurrencyCode	0	999	0	CC_key
GAC	0	32	0	codevalue_list
ICA_BIN	0	32	0	codevalue_list
Availment	0	100	0	percent
Card age	0	100	0	days
Card limit	0	20000	0	Euro
KI_Range	0	32	0	codevalue_list
Last answer	0	45	45	days
Last GAA	0	45	0	days
Last Referral	0	45	45	days
Client	0	32	0	codevalue_list
Merchant_ID	0	32	0	codevalue_list
Panic factor	0	100	0	percent
POS_Entry	0	32	0	POS_Entry_Mode
Terminal_ID	0	32	0	codevalue_list
Z01	0	32	0	number
Z02	0	32	0	number
Z03	0	32	0	number
Z04	0	32	0	number
Z05	0	32	0	number
Z06	0	32	0	number
Z07	0	32	0	number

Z08	0	32	0	number
Z09	0	32	0	number
Z10	0	32	0	number
Z11	0	32	0	number
Z12	0	32	0	number
Time series length	0	32	0	AuthoriRequests
Decline	0	1	0	-
Case class	0	32	0	codevalue_list
Case threshold	0	1000	750	threshold
Case importance	0	1000	0	per mil
Limit	0	30000	0	Euro
RiskScore	0	1000	0	per mil

The default value is adopted by the output variable, when no rule fires for this variable. Various methods can be used for the defuzzification, which either furnish the "most plausible result" or the "best" compromise.

To the compromise-forming methods belong:
CoM (Center of Maximum)
CoA (Center of Area)
CoA BSUM, a variant for efficient VLSI implementations

The "most plausible result" is furnished by:
MoM (Mean of Maximum)
MoM BSUM, a variant for efficient VLSI implementations

The following table lists all variables linked with one interface, as well as the corresponding fuzzification or defuzzification method.

Table 4: Interfaces

Variable name	Type	Fuzzification/defuzzification

AvailBal	Input	calculate MBF
Amount	Input	calculate MBF
BranchCode	Input	calculate MBF
Branch class	Input	calculate MBF
CountryCode	Input	calculate MBF
CurrencyCode	Input	calculate MBF
GAC	Input	calculate MBF
ICA_BIN	Input	calculate MBF
Availment	Input	calculate MBF
Card age	Input	calculate MBF
Card limit	Input	calculate MBF
KI_Range	Input	calculate MBF
Last answer	Input	calculate MBF
Last GAA	Input	calculate MBF
Last Referral	Input	calculate MBF
Client	Input	calculate MBF
Merchant_ID	Input	calculate MBF
Panic factor	Input	calculate MBF
POS_Entry	Input	calculate MBF
Terminal_ID	Input	calculate MBF
Z01	Input	calculate MBF
Z02	Input	calculate MBF
Z03	Input	calculate MBF
Z04	Input	calculate MBF
Z05	Input	calculate MBF
Z06	Input	calculate MBF
Z07	Input	calculate MBF
Z08	Input	calculate MBF
Z09	Input	calculate MBF
Z10	Input	calculate MBF
Z11	Input	calculate MBF
Z12	Input	calculate MBF
Time series length	Input	calculate MBF
Decline	Output	MoM
Case class	Output	MoM
Case threshold	Output	default
Case importance	Output	CoM
Limit	Output	MoM
RiskScore	Output	CoM

Rule blocks

The controller behavior in the various process situations is fixed by the rule blocks. Each single rule block contains rules for a fixed set of input and output variables.

The "IF" part of the rules thereby describes the situation in which the rule is supposed to be valid; the "THEN" part describes the reaction thereto. By the "Degree of Support" (DoS), the single rules can be imparted a varying weighting.

For evaluating the rules, the "IF" part is first calculated. Hereby, various methods can be used, which are fixed by the operator type of the rule block. The operator can be of the MIN-MAX, MIN-AVG or GAMMA type. The operator behavior is in addition influenced by a parametrization.

For example:

MIN-MAX having the parameter value 0	=	Minimum-Operator (MIN).
MIN-MAX having the parameter value 1	=	Maximum-Operator (MAX).
GAMMA, having the parameter value 0	=	Product-Operator (PROD).

The Minimum-Operator is the generalization of the Boolean "AND", and the Maximum-Operator is the generalization of the Boolean "OR".

The results of the single rules are summarized in the subsequent fuzzy composition to overall conclusions. The BSUM method hereby considers all rules firing for one condition, whereas the MAX method takes only dominant rules into account.

Translation of claims filed January 11, 2002

CLAIMS

1. A method which is implemented on a computer and which is provided for identifying and determining fraudulent transaction data in a computer-controlled transaction processing system comprising a prediction model for receiving current transaction data, for processing the current transaction data, and for outputting at least one output value that depicts a probability of a fraudulent transaction, wherein, on the basis of stored data, for

- a time series analysis and
- expert rules concerning parameters which occur in a statistically significant cumulative manner during fraudulent transactions, especially with respect to the origin of the means of payment/user, to the branch and to the beneficiary of the transaction, as well as to the magnitude or value of the transaction, the evaluation is carried out by means of the prediction model with respect to the risk of the current transaction being fraudulent, and a corresponding output value is generated,

wherein the prediction model combines a limit, which is essentially based on the expert rules and which is specific for the type of transaction, with a value, which is essentially based on the time series analysis of preceding transactions with regard to the same means of payment, and which is specific for the current transaction, in order to generate the output value,

the combination being carried out in a floating manner so that output values can be generated which vary according to the extent of the suspicion of misuse and which can be used to initiate reactions of different magnitude to the current transaction request instead of the definition of only one risk threshold for authorization of the transaction.

2. The method according to claim 1, wherein the time series analysis is implemented in the form of fuzzy logic rules.

3. The method according to claim 1 or 2, wherein the expert rules are implemented in the form of fuzzy logic rules.

Abstract

The invention relates to a method which is implemented on a computer and which is provided for identifying and determining fraudulent transaction data in a computer controlled transaction processing system comprising a prediction model for receiving current transaction data, for processing the current transaction data, and for outputting at least one output value that depicts a probability of a fraudulent transaction. According to the invention, the prediction model is used to carry out the evaluation with regard to the risk that the current transaction is fraudulent, and a corresponding output value is generated. This evaluation is carried out using stored data of a time series analysis of earlier transactions with respect to the same means of payment or user and to expert rules concerning parameters which occur in a statistically significant cumulative manner during fraudulent transactions, especially with respect to the origin of the means of payment/user, to the branch and to the beneficiary of the transaction, as well as to the magnitude or value of the transaction. The prediction model combines a limit, which is essentially based on the expert rules and which is specific for the type of transaction, with a value, which is essentially based on the time series analysis and which is specific for the current transaction, in order to generate the output value. The combination is carried out in a floating manner so that output values can be generated which vary according to the extent of the suspicion of misuse and which can be used to initiate different reactions to the current transaction request

FIG.1

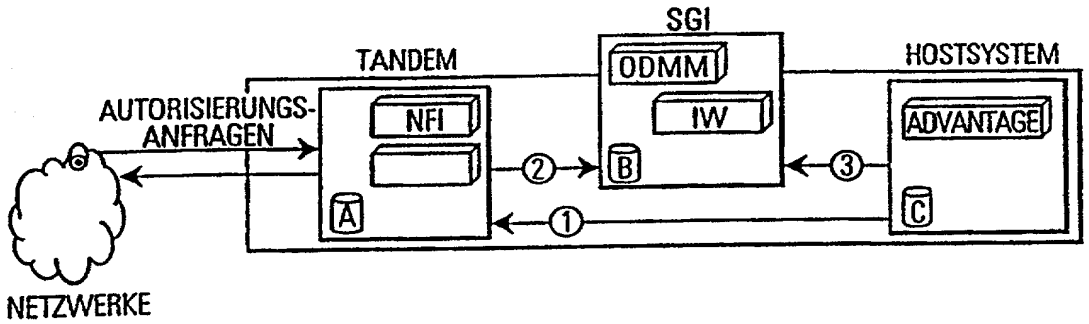


FIG.2

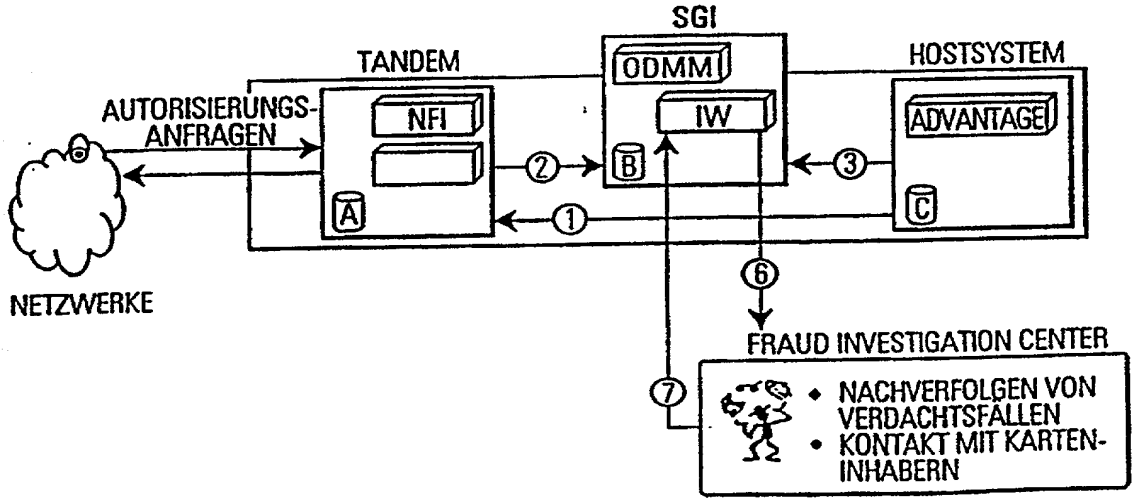


FIG.3

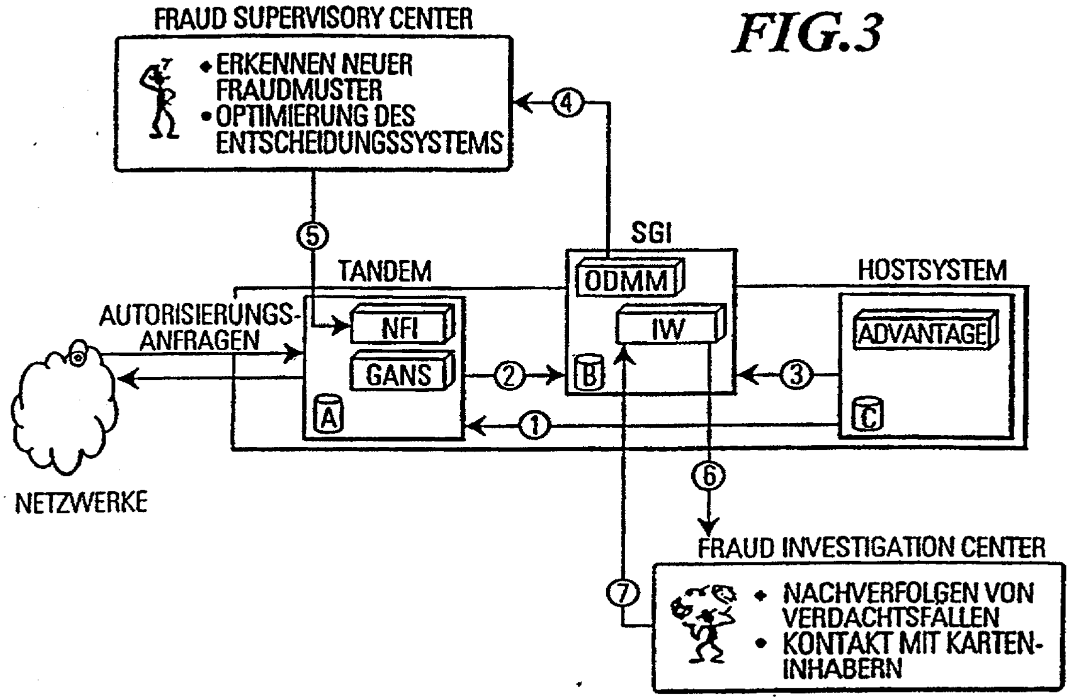
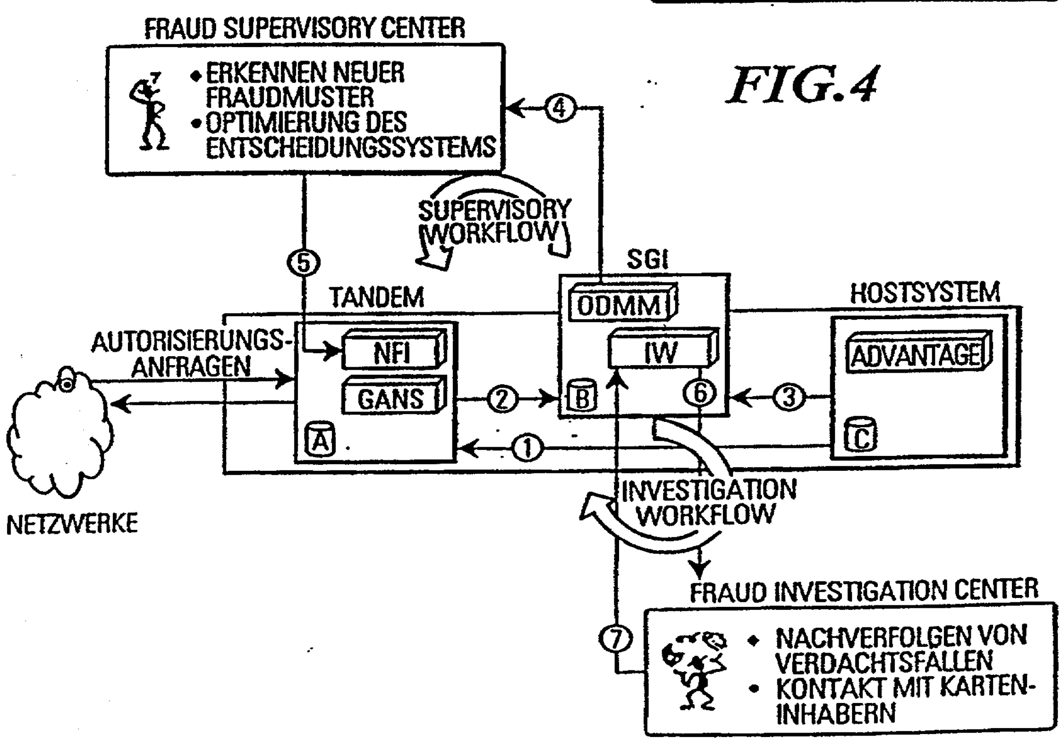
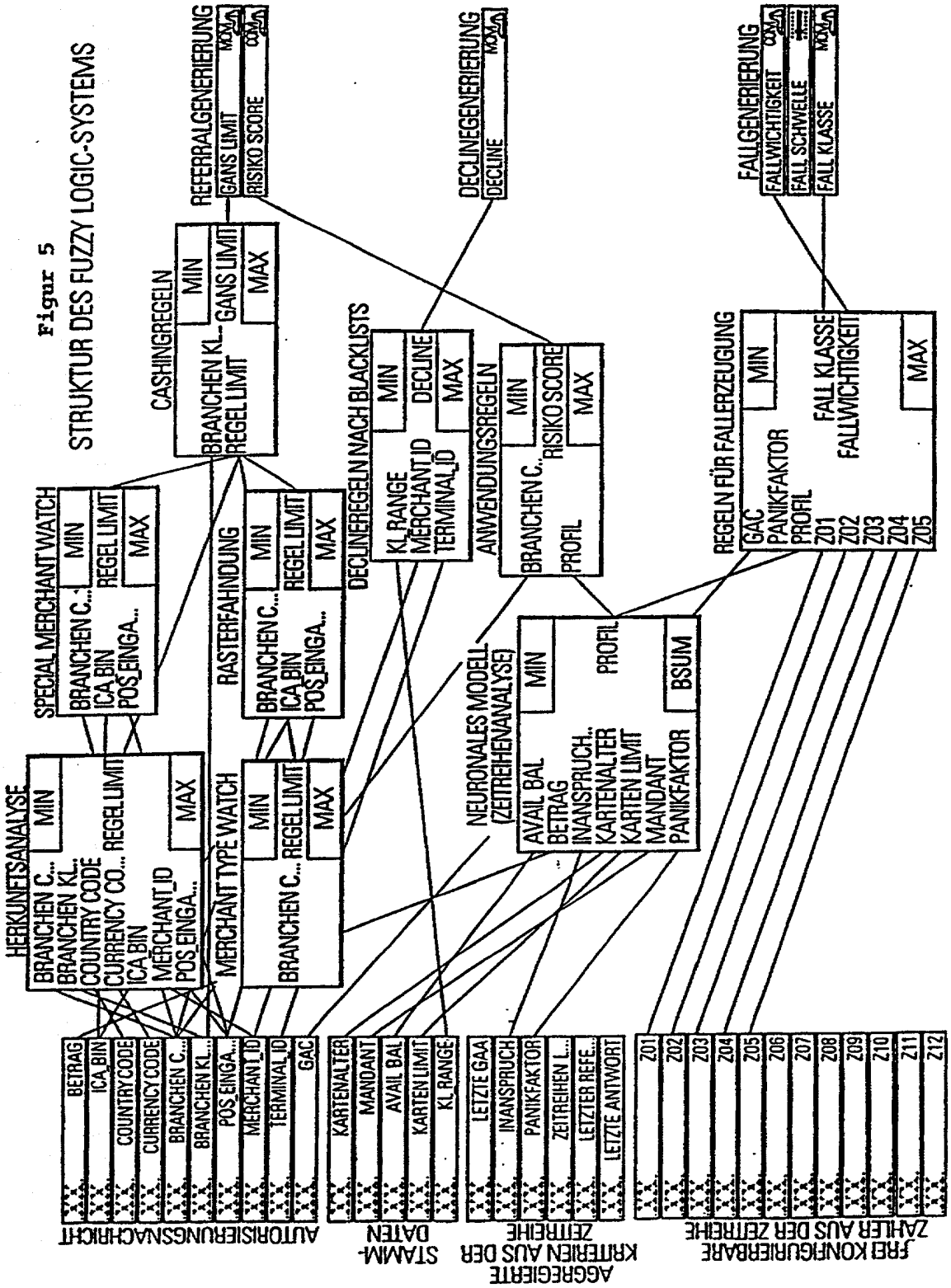


FIG.4



Figur 5

STRUKTUR DES FUZZY LOGIC-SYSTEMS



DECLARATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **EXPERT SYSTEM, the specification of which was filed as International Application PCT/EP00/08516 on** August 31, 2000;

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

Number	Country filed	Day/month/year	Priority Claimed Under 35 USC 119
199 41 868.3	Fed. Rep. of Germany	2 September 1999	Yes

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful and false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor: **Constantin VON ALTROCK**

Inventor's Signature: _____

Date: 2002-02-26

Residence: Baumgartsweg 22
52076 Aachen
Federal Republic of Germany

Citizenship: Federal Republic of Germany

Post Office Address: Same as above.

Inventor: **Hanns Michael HEPP**

Inventor's Signature: *[signature]*

Date: 2002 - 3 - 5

Residence: Adolf-Guckes-Weg 1
65817 Eppstein
Federal Republic of Germany

Citizenship: Federal Republic of Germany

Post Office Address: Same as above.

10070490.052102

Inventor: **Johann PRASCHINGER**

Inventor's Signature: ______________________

Date: 4. 3. 2002

Residence: Am Heegwald 60
61381 Friedrichsdorf
Federal Republic of Germany

Citizenship: Federal Republic of Germany

Post Office Address: Same as above.